REMOTE SECURITY MONITORING METHOD

Patent Number: JP11053669

Publication date: 1999-02-26

Inventor(s): KAWAKUBO HIDEJI; YAMANAKA KIYOSHI; OKUGAWA MORIFUMI

Applicant(s):: NIPPON TELEGR & TELEPH CORP <NTT>

Requested Patent: ☐ JP11053669

Application Number: JP19970209526 19970804

Priority Number(s):

IPC Classification: G08B25/08 ; G08B29/06 ; H04L12/02 ; H04L29/10 ; H04M11/04 ; H04Q9/00

EC Classification:

Equivalents:

Abstract

PROBLEM TO BE SOLVED: To quickly locate, at a security monitoring center without the need of using a private communication channel, a security monitoring device where security monitoring information is generated from among a large number of such devices for customers joining the above center which are installed far away from the center.

SOLUTION: A security monitoring center A and many security monitoring devices Bi for customers are respectively connected through an ISDN communication channel network M. The above arrangement, if security monitoring information Fi is generated in anyone of the security monitoring device Bi for the customers, the information is automatically sent out to the security monitoring center A through the ISDN communication channel network M along with attribute information (subscriber number) Ni. In the security monitoring center A, the sent-out security monitoring information Fi and the attribute information Ni are received, thus it is possible to locate/monitor any security monitoring device which has generated the security monitoring information from among a large number of such devices Bi for the customers.

(19)日本国特許庁（JP） (12) 公 開 特 許 公 報 （A） (11)特許出願公開番号

特開平11-53669

(43)公開日　平成11年(1999) 2 月26日

(51)Int.Cl.⁶　　　　　　　　　識別記号　　　　　　　FI
　G08B　25/08　　　　　　　　　　　　　　　G08B　25/08　　　　　E
　　　　　29/06　　　　　　　　　　　　　　　　　　　29/06
　H04L　12/02　　　　　　　　　　　　　　H04M　11/04
　　　　　29/10　　　　　　　　　　　　　　H04Q　9/00　　　　311J
　H04M　11/04　　　　　　　　　　　　　　H04L　11/02　　　　Z

審査請求　未請求　請求項の数8　OL　（全 9 頁）　最終頁に続く

(21)出願番号　特願平9-209526

(22)出願日　平成 9 年(1997) 8 月 4 日

(71)出願人　000004226
　　　　　　日本電信電話株式会社
　　　　　　東京都新宿区西新宿三丁目19番 2 号
(72)発明者　河久保　秀二
　　　　　　東京都新宿区西新宿 3 丁目19番 2 号　日本
　　　　　　電信電話株式会社内
(72)発明者　山中　喜義
　　　　　　東京都新宿区西新宿 3 丁目19番 2 号　日本
　　　　　　電信電話株式会社内
(72)発明者　奥川　守文
　　　　　　東京都新宿区西新宿 3 丁目19番 2 号　日本
　　　　　　電信電話株式会社内
(74)代理人　弁理士　田中　正治

(54)【発明の名称】　遠隔セキュリティ監視法

(57)【要約】
【課題】　セキュリティ監視センタで、それに加入し且つそれとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置中のいずれにセキュリティ監視情報が発生したのかを、専用の通信回線を用いる必要なしに、速やかに監視できるようにする。
【解決手段】　セキュリティ監視センタと多数の顧客用セキュリティ監視装置のそれぞれとを、ISDN通信回線網を介して結び、各顧客用セキュリティ監視装置にセキュリティ監視情報が発生した場合、それを、セキュリティ監視センタに、ISDN通信回線網を介して属性情報とともに自動的に送出させ、セキュリティ監視センタで、それに送出させたセキュリティ監視情報及び属性情報を受信させ、多数の顧客用セキュリティ監視装置中のいずれの顧客用セキュリティ監視装置でセキュリティ監視情報が発生したのかを監視可能にさせる。

セキュリティ監視センタA　　ISDN通信回線網M　　顧客用セキュリティ監視装置D

属性情報（加入番号）Nᵢ＋セキュリティ監視情報Fᵢ
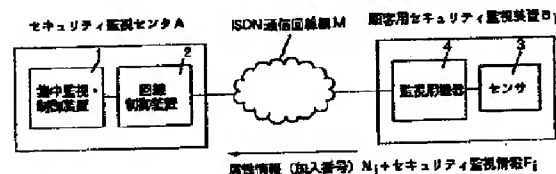
【特許請求の範囲】

【請求項1】セキュリティ監視センタに、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置を加入させ、

上記セキュリティ監視センタと上記多数の顧客用セキュリティ監視装置のそれぞれとをISDN通信回線網を介して結び、

上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、当該顧客用セキュリティ監視装置のセキュリティ監視情報が発生した場合、当該セキュリティ監視情報を、上記セキュリティ監視センタに、上記ISDN通信回線網を介して、当該顧客用セキュリティ監視装置の属性情報とともに自動的に送出させるようにし、

上記セキュリティ監視センタにおいて、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して自動的に送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を受信させ、上記多数の顧客用セキュリティ監視装置中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを監視可能にさせるようにしたことを特徴とする遠隔セキュリティ監視法。

【請求項2】請求項1記載の遠隔セキュリティ監視法において、

上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、当該顧客用セキュリティ監視装置の作動検査用情報を、上記セキュリティ監視センタに、上記ISDN通信回線網を介して、定期的に、自動的に送出させるようにし、

上記セキュリティ監視センタにおいて、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して定期的に自動的に送出させた当該顧客用セキュリティ監視装置の作動検査用情報を受信させ、当該セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに自動的に上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を正常に受信するか否かを、定期的に監視可能にさせるようにしたことを特徴とする遠隔セキュリティ監視法。

【請求項3】請求項2記載の遠隔セキュリティ監視法において、

上記セキュリティ監視センタにおいて、当該セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して定期的に自動的に送出させた当該顧客用セキュリティ監視装置の作動検査用情報を受信した場合、その受信に基づき、当該顧客用セキュリティ監視装置の切断用情報を、当該顧客用セキュリティ監視装置に、上記ISDN通信回線網を介して送出させるよ

うにし、

上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、上記セキュリティ監視センタが当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置の切断用情報を受信させ、当該顧客用セキュリティ監視装置が上記セキュリティ監視センタに上記ISDN通信回線網を介して当該顧客用セキュリティ監視装置の作動検査用情報を定期的に自動的に送出させた状態の切断をさせるようにしたことを特徴とする遠隔セキュリティ監視法。

【請求項4】請求項1記載の遠隔セキュリティ監視法において、

上記セキュリティ監視センタにおいて、当該セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して自動的に送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を受信した場合、その受信に基づき、当該顧客用セキュリティ監視装置の制御用情報を、当該顧客用セキュリティ監視装置に、上記ISDN通信回線網を介して送出させるようにし、

上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、セキュリティ監視センタが当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置の制御用情報を受信させ、そのようにさせることで、当該顧客用セキュリティ監視装置を当該顧客用セキュリティ監視装置の制御用情報の内容に応じて作動させるようにしたことを特徴とする遠隔セキュリティ監視法。

【請求項5】請求項1記載の遠隔セキュリティ監視法において、

上記多数の顧客用セキュリティ監視装置のそれぞれが、当該顧客用セキュリティ監視装置のセキュリティ監視情報を、上記ISDN通信回線網を介して、上記セキュリティ監視センタに、当該顧客用セキュリティ監視装置の属性情報とともに自動的に送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT－Q931）で規定されたユーザ・ユーザ間信号（UUI：User－to－User signalling）形態を利用することを特徴とする遠隔セキュリティ監視法。

【請求項6】請求項2記載の遠隔セキュリティ監視法において、

上記多数の顧客用セキュリティ監視装置のそれぞれが、当該顧客用セキュリティ監視装置の作動検査用情報を上記セキュリティ監視センタに上記ISDN通信回線網を介して送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT－Q931）で規定されたユーザ・ユーザ間信号（UUI：User－to－User signalling）形態を利用するこ

とを特徴とする遠隔セキュリティ監視法。

【請求項7】請求項3記載の遠隔セキュリティ監視法において、

上記セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置の作動検査用情報を受信したのに基づき、当該顧客用セキュリティ監視装置の切断用情報を当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User　signalling）形態を利用することを特徴とする遠隔セキュリティ監視法。

【請求項8】請求項4記載の遠隔セキュリティ監視法において、

セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を受信したのに基づき、当該顧客用セキュリティ監視装置の制御用情報を当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User　signalling）形態を利用することを特徴とする遠隔セキュリティ監視法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、セキュリティ監視センタにおいて、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを監視できるようにした遠隔セキュリティ監視法に関する。

【0002】

【従来の技術】従来、図5に示すような、全域的にまたは各地域的に設置されたセキュリティ監視センタAと、それとは遠隔な位置にそれぞれ顧客の監視圏（建物、庭園など）内において設置された多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち、顧客用セキュリティ監視装置B_i（i＝1、2………）とを、顧客用セキュリティ監視装置B_iに専用の通信回線L_iによって結び、顧客用セキュリティ監視装置B_iにおいて、セキュリティ監視情報F_iが発生した場合、そのセキュリティ監視情報F_iをセキュリティ監視センタAに専用の通信回線L_iを介して送出させるようにし、また、セキュリティ監視センタAにおいて、顧客用セキュ

リティ監視装置B_iがセキュリティ監視センタAに専用の通信回線L_iを介して送出させたセキュリティ監視情報F_iを受信させ、顧客用セキュリティ監視装置B_iにセキュリティ監視情報F_iが発生したことを監視可能にさせるようにした遠隔セキュリティ監視法が提案されている。

【0003】このような従来の遠隔セキュリティ監視法によれば、セキュリティ監視センタAにおいて、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置B_1、B_2………中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを、監視できることは明らかである。

【0004】

【発明が解決しようとする課題】上述した従来の遠隔セキュリティ監視法による場合、顧客用セキュリティ監視装置B_iに専用の通信回線L_iを用意する必要があり、上述した監視を行うのに設備費がかさむなどの欠点を有していた。よって、本発明は、上述した欠点のない、新規な遠隔セキュリティ監視法を提案せんとするものである。

【0005】

【課題を解決するための手段】本願第1番目の発明による遠隔セキュリティ監視法は、（i）セキュリティ監視センタに、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置を加入させ、（ii）上記セキュリティ監視センタと上記多数の顧客用セキュリティ監視装置のそれぞれとをISDN通信回線網を介して結び、（iii）上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、当該顧客用セキュリティ監視装置のセキュリティ監視情報が発生した場合、当該セキュリティ監視情報を、上記セキュリティ監視センタに、上記ISDN通信回線網を介して、当該顧客用セキュリティ監視装置の属性情報とともに自動的に送出させるようにし、上記セキュリティ監視センタにおいて、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して自動的に送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を受信させ、上記多数の顧客用セキュリティ監視装置中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを監視可能にさせるようにする。この場合、上記多数の顧客用セキュリティ監視装置のそれぞれが、当該顧客用セキュリティ監視装置のセキュリティ監視情報を、上記ISDN通信回線網を介して、上記セキュリティ監視センタに、当該顧客用セキュリティ監視装置の属性情報とともに自動的に送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User　signalling）形態を利用するのを可とする。

【0006】本願第2番目の発明による遠隔セキュリティ監視法は、（i）上述した本願第1番目の発明による遠隔セキュリティ監視法において、（ii）上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、当該顧客用セキュリティ監視装置の作動検査用情報を、上記セキュリティ監視センタに、上記ISDN通信回線網を介して、定期的に、自動的に送出させるようにし、（iii）上記セキュリティ監視センタにおいて、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して定期的に自動的に送出させた当該顧客用セキュリティ監視装置の作動検査用情報を受信させ、当該セキュリティ監視センタがく上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに自動的に上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を正常に受信するか否かを、定期的に監視可能にさせるようにする。この場合、上記多数の顧客用セキュリティ監視装置のそれぞれが、当該顧客用セキュリティ監視装置の作動検査用情報を上記セキュリティ監視センタに上記ISDN通信回線網を介して送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User signalling）形態を利用することを可とする。

【0007】本願第3番目の発明による遠隔セキュリティ監視法は、（i）上述した本願第2番目の発明による遠隔セキュリティ監視法において、（ii）上記セキュリティ監視センタにおいて、当該セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して定期的に自動的に送出させた当該顧客用セキュリティ監視装置の作動検査用情報を受信した場合、その受信に基づき、当該顧客用セキュリティ監視装置の切断用情報を、当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出させるようにし、（iii）上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、上記セキュリティ監視センタが当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置の切断用情報を受信させ、そのようにさせることで、当該顧客用セキュリティ監視装置が上記セキュリティ監視センタに上記ISDN通信回線網を介して当該顧客用セキュリティ監視装置の作動検査用情報を定期的に自動的に送出させた状態の切断をさせるようにする。この場合、上記セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置の作動検査用情報を受信したのに基づき、当該顧客用セキュリティ監視装置の切断用情報

を当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User signalling）形態を利用するのを可とする。

【0008】本願第4番目の発明による遠隔セキュリティ監視法は、（i）上述した本願第1番目の発明による遠隔セキュリティ監視法において、（ii）上記セキュリティ監視センタにおいて、当該セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して自動的に送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を受信した場合、その受信に基づき、当該顧客用セキュリティ監視装置の制御用情報を、当該顧客用セキュリティ監視装置に、上記ISDN通信回線網を介して送出させるようにし、（iii）上記多数の顧客用セキュリティ監視装置のそれぞれにおいて、セキュリティ監視センタが当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置の制御用情報を受信させ、当該顧客用セキュリティ監視装置を当該顧客用セキュリティ監視装置の制御用情報の内容に応じて作動させるようにする。この場合、セキュリティ監視センタが、上記多数の顧客用セキュリティ監視装置のそれぞれが当該セキュリティ監視センタに上記ISDN通信回線網を介して送出させた当該顧客用セキュリティ監視装置のセキュリティ監視情報及び属性情報を受信したのに基づき、当該顧客用セキュリティ監視装置の制御用情報を、当該顧客用セキュリティ監視装置に上記ISDN通信回線網を介して送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User signalling）形態を利用するのを可とする。

【0009】
【発明の実施の形態1】次に、図1を伴って、本発明による遠隔セキュリティ監視法の第1の実施の形態を、セキュリティ監視の対象が、顧客の監視圏（建物、庭園など）内への不法侵入であるとして、述べよう。

【0010】図1に示す本発明による遠隔セキュリティ監視法の第1の実施の形態においては、全地域的にまたは各地域的に設置されたセキュリティ監視センタAに、それとは遠隔な位置にそれぞれ顧客の監視圏内において設置された多数の顧客用セキュリティ監視装置B_1、B_2………を加入させ、そして、セキュリティ監視センタAと、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_i（i＝1、2………）とを、ISDN通信回線網Mをによって結ぶ、

【0011】この場合、セキュリティ監視センタAは、ISDN通信回線網Mに接続している回線制御装置1と、それに接続されている集中監視・制御装置2とを有する。また、顧客用セキュリティ監視装置B_iは、ISDN通信回線網Mに接続しているとともに、顧客の監視圏内への不法侵入を検出するセンサ3を接続している監視用機器4を有する。

【0012】そして、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_iにおいて、そのセンサ3が顧客の監視圏内への不法侵入を検出することによって、監視用機器4に、当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_iが発生した場合、そのセキュリティ監視情報F_iを、セキュリティ監視センタAに、ISDN通信回線網Mを介して、当該顧客用セキュリティ監視装置B_iの属性情報N_i（例えば、ISDN通信回線網Mで得られる当該顧客用セキュリティ監視装置B_iのISDN通信回線網Mへの加入番号）とともに、自動的に送出させるようにする。

【0013】ここで、上述した多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち、顧客用セキュリティ監視装置B_iが、当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_iを、ISDN通信回線網Mを介して、セキュリティ監視センタAに、当該顧客用セキュリティ監視装置B_iの属性情報N_iとともに自動的に送出するのに、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User signalling）形態を利用する。

【0014】また、セキュリティ監視センタAにおいて、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタAにISDN通信回線網Mを介して自動的に送出させた当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び当該顧客用セキュリティ監視装置B_iの属性情報N_iを、回線制御装置1を介して集中監視・制御装置2に供給する態様で受信させ、集中監視・制御装置2を用いて、多数の顧客用セキュリティ監視装置B_1、B_2………中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのか（この場合、当該顧客用セキュリティ監視装置B_iにおいてセキュリティ監視情報F_iが発生したこと）を監視可能にさせるようにする。

【0015】以上で、本発明による遠隔セキュリティ監視法の第1の実施の形態が明らかとなった。

【0016】このような本発明による遠隔セキュリティ監視法の第1の実施の形態によれば、セキュリティ監視センタAにおいて、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置B_1、B_2………中の

いずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを、顧客用セキュリティ監視装置B_iに専用の通信回線を用いる必要なしに、従って設備費がかさむことなしに、的確に且つ速やかに、監視できることは明らかである。

【0017】
【発明の実施の形態2】次に、図2を伴って、本発明による遠隔セキュリティ監視法の実施の形態を述べよう。図2に示す本発明による遠隔セキュリティ監視法の第2の実施の形態は、図1に示す本発明による遠隔セキュリティ監視法の第1の実施の形態において、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_iにおいて、当該顧客用セキュリティ監視装置B_iの監視用機器4がそれに接続されているセンサ3が正常に動作していることの確認を行った下で、当該顧客用セキュリティ監視装置B_iの作動検査用情報Q_i（当該顧客用セキュリティ監視装置B_iのISDN通信回線網Mへの加入番号）を、セキュリティ監視センタAに、ISDN通信回線網Mを介して、定期的に、自動的に送出させるようにする。

【0018】ここで、上述した多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち、顧客用セキュリティ監視装置B_iが、当該顧客用セキュリティ監視装置B_i用の作動検査用情報Q_iを、当該セキュリティ監視センタAにISDN通信回線網Mを介して定期的に自動的に送出するのに、本発明による遠隔セキュリティ監視法の第1の実施の形態で上述したセキュリティ監視情報F_i及び属性情報N_iを自動的に送出する場合と同様に、ISDNユーザ・網インタフェース　レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User signalling）形態を利用する。

【0019】また、セキュリティ監視センタAにおいて、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタAにISDN通信回線網Mを介して定期的に自動的に送出させた当該顧客用セキュリティ監視装置B_iの作動検査用情報Q_iを、回線制御装置1を介して集中監視・制御装置2に供給する態様で受信させ、集中監視・制御装置2を用い、当該セキュリティ監視センタAが、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれすなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタAにISDN通信回線網Mを介して送出させた当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び当該顧客用セキュリティ監視装置B_iの属性情報N_i（加入番号）を、正常に受信するか否かを（当該セキュリティ監視センタAが作動検査用情報Q_iを正常に受信している場合、正常に受信することを、正常に受信していない場合、正常に受信していないことを）、定期的

に監視可能にさせるようにする。

【００２０】以上が、本発明による遠隔セキュリティ監視法の第２の実施の形態である。このような本発明による遠隔セキュリティ監視法の第２の実施の形態によれば、上述した本発明による遠隔セキュリティ監視法の第１の実施の形態の場合と同様に、セキュリティ監視センタＡにおいて、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置B_1、B_2………中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを、顧客用セキュリティ監視装置B_iに専用の通信回線を用いる必要なしに、従って設備費がかさむことなしに、的確に且つ速やかに、監視できることは明らかであるとともに、そのような監視を、セキュリティ監視センタＡにおいて、当該セキュリティ監視センタＡが、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれすなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタＡにＩＳＤＮ通信回線網Ｍを介して送信させた当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び属性情報N_iを正常に受信するか否かを、定期的に監視可能にさせるようにしていることから、高い信頼性を以って行うことができる。

【００２１】

【発明の実施の形態３】次に、図３を伴って、本発明による遠隔セキュリティ監視法の第３の実施の形態を述べよう。

【００２２】図３に示す本発明による遠隔セキュリティ監視法の第３の実施の形態は、図２に示す本発明による遠隔セキュリティ監視法の第２の実施の形態において、セキュリティ監視センタＡにおいて、当該セキュリティ監視センタＡが、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれすなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタＡにＩＳＤＮ通信回線網Ｍを介して定期的に自動的に送出させた当該顧客用セキュリティ監視装置B_iの作動検査用情報Q_iを受信した場合、その受信に基づき、当該顧客用セキュリティ監視装置B_iの切断用情報K_iを、当該顧客用セキュリティ監視装置B_iにＩＳＤＮ通信回線網Ｍを介して送出させるようにする。

【００２３】ここで、セキュリティ監視センタＡが、顧客用セキュリティ監視装置B_iの切断用情報K_iを顧客用セキュリティ監視装置B_iにＩＳＤＮ通信回線網Ｍを介して送出させるのに、本発明による遠隔セキュリティ監視法の第２の実施の形態で上述した顧客用セキュリティ監視装置B_iの作動検査用情報Q_iを定期的に自動的に送出する場合と同様に、ＩＳＤＮユーザ・網インターフェース　レイヤ３仕様で規定されたユーザ・ユーザ間信号形態を利用する。

【００２４】また、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち、顧客用セキュ

リティ監視装置B_iにおいて、セキュリティ監視センタＡが当該顧客用セキュリティ監視装置B_iにＩＳＤＮ通信回線網Ｍを介して送出させた当該顧客用セキュリティ監視装置B_iの切断用情報K_iを受信させ、当該顧客用セキュリティ監視装置B_iがセキュリティ監視センタＡにＩＳＤＮ通信回線網Ｍを介して当該顧客用セキュリティ監視装置B_iの作動検査用情報Q_iを定期的に自動的に送出させた状態（当該顧客用セキュリティ監視装置B_iがＩＳＤＮ通信回線網Ｍを介してセキュリティ監視センタＡに情報を送出させ得る回線オンの状態）の切断をさせるようにする。

【００２５】以上が、本発明による遠隔セキュリティ監視法の第３の実施の形態である。このような本発明による遠隔セキュリティ監視法の第３の実施の形態によれば、本発明による遠隔セキュリティ監視法の第２の実施の形態で上述した作用・効果を得ることができることは明らかであるとともに、当該顧客用セキュリティ監視装置B_iがセキュリティ監視センタＡにＩＳＤＮ通信回線網Ｍを介して当該顧客用セキュリティ監視装置B_iの作動検査用情報Q_iを定期的に自動的に送出させた状態の切断を、できる限り速やかにさせることで、セキュリティ監視センタＡが、顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタＡにＩＳＤＮ通信回線網Ｍを介して顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び属性情報N_iを正常に受信するか否かの定期的な監視を、ＩＳＤＮ通信回線網Ｍの短い使用時間（例えば課金対象時間外時間）で効果的に行わせることができる。

【００２６】

【発明の実施の形態４】次に、図４を伴って、本発明による遠隔セキュリティ監視法の第４の実施の形態を述べよう。図４に示す本発明による遠隔セキュリティ監視法の第４の実施の形態は、図１に示す本発明による遠隔セキュリティ監視法の第１の実施の形態において、セキュリティ監視センタＡにおいて、当該セキュリティ監視センタＡが、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタＡにＩＳＤＮ通信回線網Ｍを介して自動的に送出させた当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び当該顧客用セキュリティ監視装置B_iの属性情報（加入番号）N_iを、回線制御装置１を介して集中監視・制御装置２に供給する態様で受信した場合、その受信に基づき、当該顧客用セキュリティ監視装置B_iの制御用情報C_iを、当該顧客用セキュリティ監視装置B_iに、回線制御装置１を介し、次でＩＳＤＮ通信回線網Ｍを介して、当該顧客用セキュリティ監視装置B_iが当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び当該顧客用セキュリティ監視装置B_iの属性情報（加入番号）N_iを送出するのに用いたチャンネルとは

別のチャンネルを用いて、集中監視・制御装置2から、送出させるようにする。

【0027】ここで、セキュリティ監視センタAが、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれすなわち顧客用セキュリティ監視装置B_iが当該セキュリティ監視センタAにISDN通信回線網Mに送出させた当該顧客用セキュリティ監視装置B_iのセキュリティ監視情報F_i及び当該顧客用セキュリティ監視装置B_iの属性情報（加入番号）N_iを受信した場合に、その受信に基づき、当該顧客用セキュリティ監視装置B_iの制御用情報C_iを当該セキュリティ監視センタAにISDN通信回線網Mを介して送出させるのに、本発明による遠隔セキュリティ監視法の第1の実施の形態で上述したセキュリティ監視情報F_i及び属性情報（加入番号）N_iを自動的に送出する場合と同様に、ISDNユーザ・網インタフェース レイヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号（UUI：User−to−User signalling）形態を利用する。

【0028】また、多数の顧客用セキュリティ監視装置B_1、B_2………のそれぞれ、すなわち顧客用セキュリティ監視装置B_iにおいて、セキュリティ監視センタAが当該顧客用セキュリティ監視装置B_iにISDN通信回線網Mを介して送出させた当該顧客用セキュリティ監視装置B_iの制御用情報C_iを、当該顧客用セキュリティ監視装置B_iの監視用機器4によって受信させ、当該顧客用セキュリティ監視装置B_iを、その監視用機器4を用いて、当該顧客用セキュリティ監視装置B_iの制御用情報C_iの内容に応じて所望の態様で作動させる（監視用機器4が、警報発生手段を有するとした場合、警報を発せしめたり、撮像手段を有するとした場合、顧客の監視圏内の撮像をさせたりするなど）ようにする。

【0029】以上が、本発明による遠隔セキュリティ監視法の第4の実施の形態である。このような本発明による遠隔セキュリティ監視法の第4の実施の形態によれば、上述した本発明による遠隔セキュリティ監視法の第1の実施の形態の場合と同様に、セキュリティ監視センタAにおいて、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置B_1、B_2………中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを、顧客用セキュリティ監視装置B_iに専用の通信回線を用いる必要なしに、従って設備費がかさむことなしに、的確に且つ速やかに、監視できることは明らかであるとともに、そのような監視がなされた顧客用セキュリティ監視装置を、所望の態様で作動させるようにしていることから、当該顧客用セキュリティ監視装置の付加的な監視を行わせることができる。

【0030】
【発明の実施の形態の変型・変更】上述においては、セキュリティ監視の対象が顧客の監視圏内への不法侵入で

あるとして、本発明による遠隔セキュリティ監視法の第1〜第4の実施の形態を述べたが、上述した本発明による遠隔セキュリティ監視法の第1〜第4の実施の形態によって、セキュリティ監視の対象を顧客の監視圏内への不法侵入以外として、そのセキュリティ監視を行わせることができるようにし得ることは明らかであろう。

【0031】また、上述した本発明による遠隔セキュリティ監視法の第1〜第4の実施の形態においては、いずれも、セキュリティ監視情報F_i、作業検査用情報Q_i、切断用情報K_i、制御用情報C_iなどの情報をISDN通信回線網Mを介して送出するのに、ISDNユーザ・網インターフェース レーヤ3仕様（TTC標準JT−Q931）で規定されたユーザ・ユーザ間信号形態を利用するとしたが、他の種々の信号形態を利用するようにしてもよく、その他、本発明の精神を脱することなしに種々の変型、変更をなし得るであろう。

【0032】
【発明の効果】本発明による遠隔セキュリティ監視法によれば、①セキュリティ監視センタにおいて、それとは遠隔な位置に設置された多数の顧客用セキュリティ監視装置中のいずれの顧客用セキュリティ監視装置においてセキュリティ監視情報が発生したのかを、顧客用セキュリティ監視装置のそれぞれに専用の通信回線を用いる必要なしに、速やかに、監視でき、または②そのような監視ができるとともに、そのような監視を高い信頼性を以って得ることができ、もしくは③上記①の監視を高い信頼性を以って得ることができるための監視を、ISDN通信回線網の短い使用時間で行うことができ、または④上記①の監視ができるとともに、そのような監視がなされた顧客用セキュリティ監視装置の付加的な監視を行わせることができる。

【図面の簡単な説明】
【図1】本発明による遠隔セキュリティ監視法の第1の実施の形態を示す略線的系統図である。
【図2】本発明による遠隔セキュリティ監視法の第2の実施の形態を示す略線的系統図である。
【図3】本発明による遠隔セキュリティ監視法の第3の実施の形態を示す略線的系統図である。
【図4】本発明による遠隔セキュリティ監視法の第4の実施の形態を示す略線的系統図である。
【図5】従来の遠隔セキュリティ監視法を示す略線的系統図である。
【符号の説明】
A　　セキュリティ監視センタ
B_i　　顧客用セキュリティ監視装置
C_i　　制御用情報
F_i　　セキュリティ監視情報
K_i　　切断用情報
M　　ISDN回線網
N_i　　属性情報

Q_i　　作動検査用情報　　　　　　　　3　　センサ
1　　回線制御装置　　　　　　　　　　4　　監視用機器
2　　集中監視・制御装置

【図1】
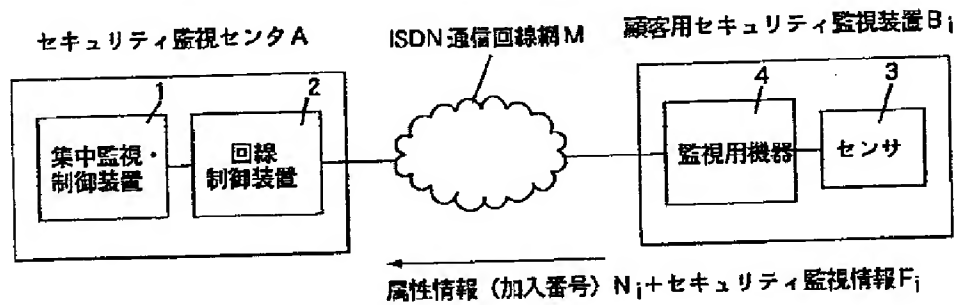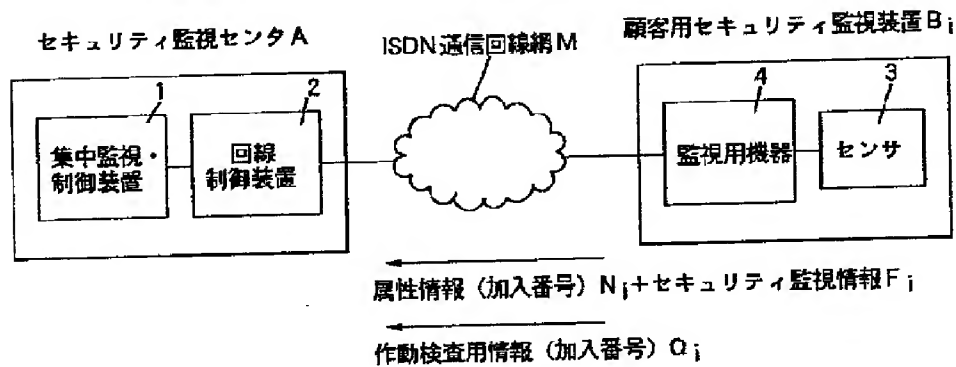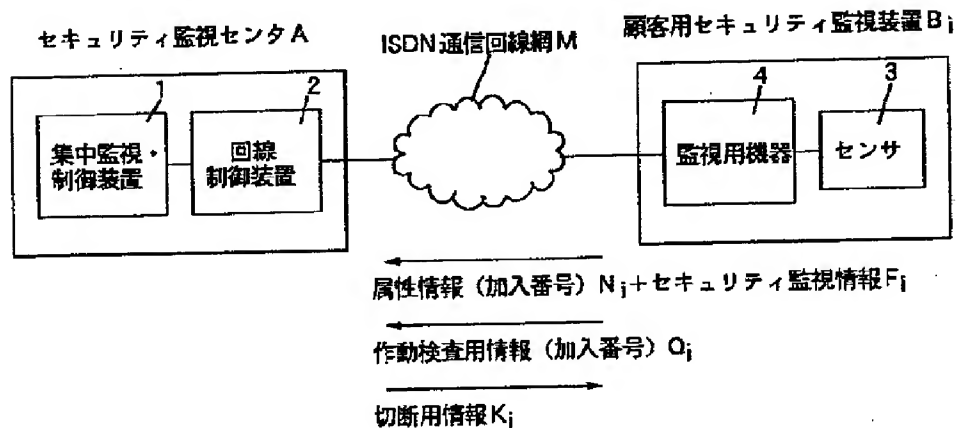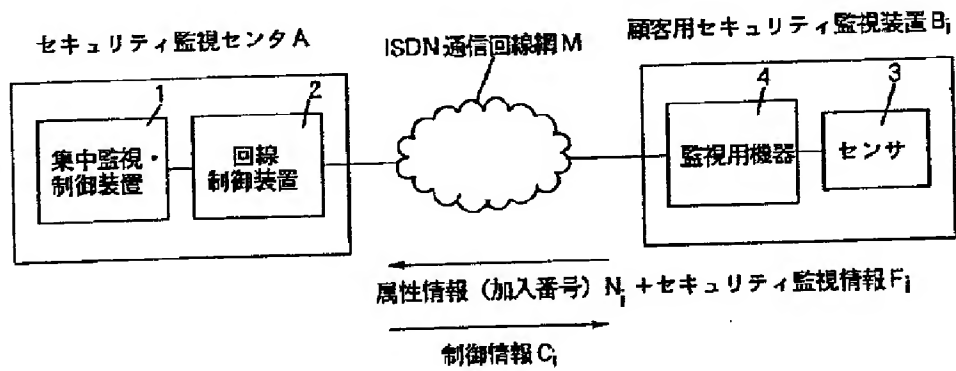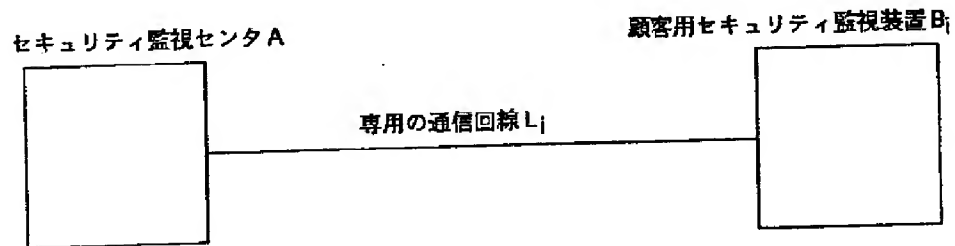
セキュリティ監視センタA　　　ISDN通信回線網M　　　顧客用セキュリティ監視装置B_i

集中監視・制御装置　回線制御装置　　監視用機器　センサ

属性情報（加入番号）N_i＋セキュリティ監視情報F_i

【図2】

セキュリティ監視センタA　　　ISDN通信回線網M　　　顧客用セキュリティ監視装置B_i

集中監視・制御装置　回線制御装置　　監視用機器　センサ

属性情報（加入番号）N_i＋セキュリティ監視情報F_i

作動検査用情報（加入番号）Q_i

【図3】

セキュリティ監視センタA　　　ISDN通信回線網M　　　顧客用セキュリティ監視装置B_i

集中監視・制御装置　回線制御装置　　監視用機器　センサ

属性情報（加入番号）N_i＋セキュリティ監視情報F_i

作動検査用情報（加入番号）Q_i

切断用情報K_i

【図4】

セキュリティ監視センタA　　ISDN通信回線網M　　顧客用セキュリティ監視装置 B_i

集中監視・制御装置　1　　回線制御装置　2　　　監視用機器　4　　センサ　3

属性情報（加入番号） N_i ＋セキュリティ監視情報 F_i

制御情報 C_i

【図5】

セキュリティ監視センタA　　　　顧客用セキュリティ監視装置 B_i

専用の通信回線 L_i

K

(51) International Patent Classification⁷: **G06F**

(21) International Application Number:
PCT/US2004/005691

(22) International Filing Date: 26 February 2004 (26.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/450,465	26 February 2003 (26.02.2003)	US
60/450,459	26 February 2003 (26.02.2003)	US
60/466,497	29 April 2003 (29.04.2003)	US
60/491,575	31 July 2003 (31.07.2003)	US
Not furnished	25 February 2004 (25.02.2004)	US

(71) Applicant *(for all designated States except US)*: WALKER DIGITAL, LLC [US/US]; 1177 High Ridge Road, Suite 128, Stamford, CT 06905 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: TEDESCO, Daniel, E. [US/US]; Two Arden Lane, Huntington, CT 06484 (US). JORASCH, James, A. [US/US]; 25 Forest Street, 5G., Stamford, CT 06901 (US). GELMAN, Geoffrey, M. [US/US]; 21 Belltown Road, Stamford, CT 06905 (US). WALKER, Jay, S. [US/US]; 260 Oscaleta Road, Ridgefield, CT 06877 (US). TULLEY, Stephen, C. [US/US]; 115 Ruane Street, Fairfield, CT 06824 (US). O'NEILL, Vincent, M. [US/US]; 235 West End Avenue, Apartment 7G, New York, NY 10023 (US). ALDERUCCI, Dean, P. [US/US]; 8 Marion Road, Westport, CT 06880 (US).

(74) Agents: ALDERUCCI, Dean, P. et al.; Innovation Strategies and Law Group, LLC, Box 17295, Stamford, CT 06905-9998 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, C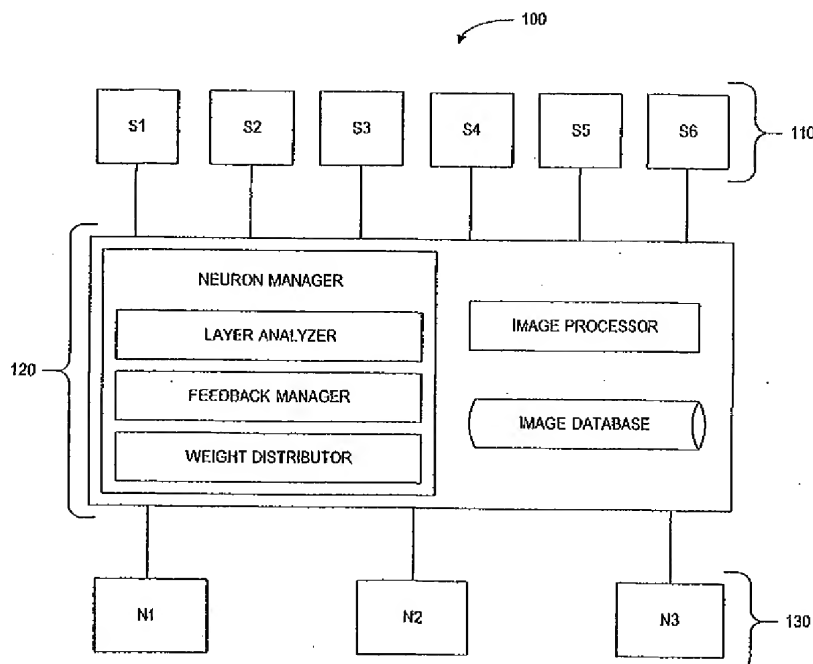H, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,

(54) Title: IMAGE ANALYSIS METHOD AND APPARATUS IN A NETWORK THAT IS STRUCTURED WITH MULTIPLE LAYERS AND DIFFERENTIALLY WEIGHTED NEURONS

(57) Abstract: Disclosed herein are systems and methods for facilitating the usage of an online workforce to remotely monitor security-sensitive sites and report potential security breaches. In some embodiments, cameras are configured to monitor critical civilian infrastructure, such as water supplies and nuclear reactors. The cameras are operatively connected to a central computer or series of computers, and images captured by the cameras are transmitted to the central computer. After initially registering with the central computer, Guardians "log on" to a central website hosted by the central computer and monitor the images, thereby earning compensation. In one embodiment, images of "no-man" zones - areas where no humans or vehicles should be present or monitored - are sent to Guardians for a simple determination of whether or not a human exists in the picture. Site owners compensate the operator of the computer system for this monitoring service, and the operator in turn compensates Guardians based on, for example, (i) the amount of time spent monitoring, and/or (ii) the degree of a given Guardian's responsiveness to real or fabricated security breaches. Among other things, systems and methods are disclosed herein for facilitating (a) the registration of monitored sites, (b) the registration of Guardians, and (c) the management of monitoring sessions, including the routing of real and fabricated images to Guardians, the rating of Guardians, and the compensation of Guardians. Many additional and alternative embodiments are contemplated, including the following example of one embodiment.

PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available):* ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMAGE ANALYSIS METHOD AND APPARATUS IN A NETWORK THAT IS STRUCTURED WITH MULTIPLE LAYERS AND DIFFERENTIALLY WEIGHTED NEURONS

5

The present utility application claims the benefit of priority of the following U.S. Provisional Patent Applications:

Application Serial No. 60/450,465, filed February 26, 2003, entitled
10 "SYSTEM AND METHOD FOR THE REMOTE MONITORING OF CRITICAL CIVILIAN INFRASTRUCTURE";

Application Serial No. 60/450,459, filed February 26, 2003, entitled "SYSTEM AND METHOD FOR THE REMOTE MONITORING OF CRITICAL
15 CIVILIAN INFRASTRUCTURE";

Application Serial No. 60/466,497, filed April 29, 2003, entitled "SYSTEM AND METHOD FOR THE PERFORMANCE AND COMPENSATION OF MICRO-TASKS"; and
20

Application Serial No. 60/491,574, filed July 31, 2003 entitled "SYSTEM AND METHOD FOR THE REMOTE MONITORING OF PRIVATE PROPERTY".

25 The present utility application is also a continuation-in-part of the following U.S. Utility Patent Application:

Application Serial No. [NOT YET ASSIGNED], filed February 25, 2004 entitled "SYSTEM FOR IMAGE ANALYSIS IN A NETWORK THAT IS
30 STRUCTURED WITH MULTIPLE LAYERS AND DIFFERENTIALLY WEIGHTED NEURONS".

Each of the above applications is incorporated by reference herein.

5   BACKGROUND

Many forms of violence and intimidation are of great concern to various
entities, ranging from individuals to nations. The United States and other
developed nations face an unprecedented challenge posed by terrorism, both
10   foreign and domestic.

The unprecedented magnitude of the threat is even worse than generally
believed, and can only be appreciated by considering the quantity and value of
other potential targets, e.g., on the U.S. homeland. In addition to the well
understood targets such as airport terminals and large commercial centers, there are
15   tens of thousands of critical infrastructure facilities in the U.S., including airport
perimeters, chemical plants, natural gas plants, pipelines and pumping stations,
nuclear and non-nuclear power plants, refineries and reservoirs.

Such facilities which are typically unguarded. Many people could, with
relative ease, approach within one hundred feet of such facilities.
20   Thus, given the magnitude of the problem posed by modern terrorism there
exists a clear and urgent need for systems and methods that to combat terrorism.

Novel data processing techniques, including image processing techniques,
may be employed in various applications to help combat terrorism.

25   DESCRIPTION OF THE DRAWINGS
FIG. 1 is an illustration of a network according to one embodiment of the
invention.

FIG. 2 is an illustration of a network according to one embodiment of the
invention.
30

DETAILED DESCRIPTION

Numerous embodiments are described in this application, and are presented for illustrative purposes only. The described embodiments are not intended to be limiting in any sense. The invention is widely applicable to numerous

5　　　embodiments, as is readily apparent from the disclosure herein.

While the methods and apparatus of the present invention are described herein by way of particular embodiments, those skilled in the art will recognize that the present invention may be practiced with modification and alteration without departing from the teachings disclosed herein. Although particular

10　　features of the present invention may be described with reference to one or more particular embodiments or figures, it should be understood that such features are not limited to usage in the one or more particular embodiments or figures with reference to which they are described.

The terms "an embodiment", "embodiment", "embodiments", "the

15　　embodiment", "the embodiments" "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more embodiments" unless expressly specified otherwise.

Further, although process steps, method steps, algorithms or the like may be described in a sequential order, such processes, methods and algorithms may be

20　　configured to work in alternate orders. In other words, any sequence or order of steps that may be described does not necessarily indicate a requirement that the steps be performed in that order.

It will be readily apparent that the various methods and algorithms described herein may be implemented by, e.g., appropriately programmed general

25　　purpose computers and computing devices. Further, programs which implement such methods and algorithms may be stored and transmitted in a variety of known media.

The steps of processes described herein may be performed in any order practical. Further, some steps may be performed simultaneously.

30　　Among the many uses of the disclosed systems and methods, Applicants have realized that there are a significant number of vulnerable sites which may be subject to hostile acts. Applicants have also realized that such sites are typically

unguarded and lack access control, and further that such access control would typically be cost prohibitive. Applications have also realized that typically people are not permitted to be at or near such sites. Applicants have also realized that very many people may be used, but are not currently being used, to perform

5   various types of productive work, especially from their homes or other convenient locations.

FIG. 1 is an illustration of a network 100 according to one embodiment of the invention. In FIG. 1, a plurality of sensors 110, such as image capture devices,

10   communicate (unidirectionally or bidirectionally) with an image processing and distribution node 120, which may also be referred to herein as a "central computer" or "central server". The image processing and distribution node 120 may also be capable of transmitting signals to sensors, either by individually addressing certain sensor(s) or by broadcasting to some or all sensors.

15   In some embodiments, if the sensor is an image capture device such as a camera, images posted from cameras may be optimized for processing / review according to various image processing rules. Such rules may function to, for example, grayscale the image, enhance brightness and/or sharpness, and/or magnify or highlight certain portions of the image. The pre-processing software

20   can be configured at the site level to tune it to the visual characteristics of a particular site (e.g. heavy sun glare at certain hours at the location the camera is viewing). The "raw" (pre-processing) image may be retained, e.g., for a site-defined time period before getting discarded.

            In an embodiment where the sensors are image capture devices, image

25   capture devices may employ on-board motion detection capabilities to trigger image capture events. In one embodiment, when an image capture event occurs, the hardware of the image capture device (also called an image capture node) will post one (or more depending on configuration) images to the image services network (e.g., the image processing and distribution node). The image capture

30   device may additionally or alternatively isolate and index a full-motion image buffer (of configurable duration before and after the triggering event), and preserve

this buffer on local storage for a finite time period (e.g., 48 hours) which is configurable.

Also, image capture devices may forward captured images to the image processing and distribution node. The image processing and distribution node may

5   preprocess the received images, and then store the (preprocessed) images. The database may create an association with the images. For example, images can be keyed in the database to the location of the images.

In some embodiments, processed images may be given a unique index number that associates them with the source site/node. Processed images may be

10   given a digital watermark and/or a digital fingerprint may be taken of the image (e.g. via an MD5 checksum) to facilitate authentication of the image in its final form.

Sensed data (e.g., images) is processed by a plurality of neurons 130 according to one or more processing algorithms described herein. Each neuron

15   processes at least one received file or data set corresponding to sensed data. The neuron in turn generates a result based on the processing.

In one embodiment, when sensed data is ready to be processed by a neuron, a request (e.g., an image review request) to process that sensed data may be posted to a routing database. The routing database may be a part of a neuron manager

20   which, among other things, controls routing of sensed data to neurons.

In one embodiment, a neuron indicates when it is ready to process by making a request (e.g., an image request). The routing database can provide the image or other sensed data to the next appropriate neuron that makes a request (e.g., an image request) based on distribution quantity and routing rules. The

25   distribution quantity and / or the routing rules can be site / node configurable.

Referring to FIG. 2, in another perspective of a network 200, neurons 130 transmit results to a results processor 210, which may be the image processing and distribution node or may be a separate device.

Each neuron has at least one respective weight that is used to evaluate the

30   processed results from that neuron. Results from neurons with lower weights may be distrusted. A weight distributor assigns weights to neurons, and updates those weights as appropriate. For example, a neuron which has generated faulty results

may be assigned reduced weight. Similarly, a neuron which has generated accurate results may be assigned a higher weight.

Also, a neuron may have more than one weight. For example, a neuron may have a different weight to represent the neuron's "accuracy" in evaluating
5　　different types of sensed data (e.g., different weights for different types of images, different weights for images vs. audio data).

Neurons are typically configured to generate extremely simple results, leading to efficient processing of results. In one embodiment, a neuron is only responsible for generating a binary result from a sensed data file. For example, a
10　　neuron may be responsible for generating a bit to represent whether or not a received image depicts a human (e.g., 1 = human present in the image, 0 = no human present in the image).

Neurons may be arranged in "layers" to provide enhanced accuracy and reliability. For example, neurons in a first layer may each have a higher weight
15　　than neurons in a second layer. In such an embodiment, neurons in the first layer may be more accurate and / or more trusted, and accordingly a neuron in the first layer could supervise one or more neurons in the second layer. It is also possible that neurons transition among layers as their weights are adjusted by the weight distributor. A layer analyzer can be used to allocate neurons to different layers,
20　　based on their weights and other criteria. The layer analyzer can also segment a layer so that different portions of a layer are used for different types of processing (e.g., different types of images, different types of sensed data)

A feedback manager can be configured to process results from neurons. The feedback manager may direct neurons to perform additional processing based
25　　on the results. For example, if a neuron processes particular sensed data (e.g., an image) to provide a "positive result" and / or a result which is believed to be atypical (e.g., human present in the image when no human should be), then the feedback manager may, for example, (i) direct the sensed data to be processed by additional neurons, e.g., in order to verify the result; (ii)
30　　　　　　Sensed data which is processed by a neuron with a relatively low weight may be directed to other neurons for redundant or additional processing.

Similarly, the number of additional neurons to which sensed data is directed may be based on the weight of the original or first neuron.

Exemplary Network Configuration

5

Embodiments of the present invention can be configured to work in a network environment whereby the central computer, the user computer and/or the monitoring device communicate with each other directly or indirectly, via a wired or wireless medium such as the Internet, LAN, WAN or Ethernet, Token Ring, or

10   via any appropriate communications means or combination of communications means. Communication between the devices and computers, and among the devices, may be direct or indirect, such as over the Internet through a Website maintained by a computer on a remote server or over an on-line data network including commercial on-line service providers, bulletin board systems and the

15   like. In yet other embodiments, the devices may communicate with one another and / or a computer over RF, cable TV, satellite links and the like.

Some, but not all, possible communication networks that may comprise the network or be otherwise part of the system include: a local area network (LAN), a wide area network (WAN), the Internet, a telephone line, a cable line, a radio

20   channel, an optical communications line, and a satellite communications link. Possible communications protocols that may be part of the system include: Ethernet (or IEEE 802.3), SAP, ATP, Bluetooth™, and TCP/IP. Further, networking of devices and computers may include use of 802.11b and related wireless protocols and/or use of cell networks (GSM and other emerging

25   standards).

Those skilled in the art will understand that computers and devices in communication with each other need not be continually transmitting to each other. On the contrary, such computers and devices need only transmit to each other as necessary, and may actually refrain from exchanging data most of the time. For

30   example, a device in communication with another device via the Internet may not transmit data to the other device for weeks at a time.

7

In an embodiment, a central computer may not be necessary and / or preferred. For example, the present invention may, in one or more embodiments, be practiced on a monitoring device in communication only with one or more user computers. In such an embodiment, any functions described as performed by the

5   central computer or data described as stored on the central computer may instead be performed by or stored on one or more monitoring devices or user computers.

Network Security

10   Communication among computers and devices may be encrypted to ensure privacy and prevent fraud in any of a variety of ways well known in the art. Appropriate cryptographic protocols for bolstering system security are described in Schneier, APPLIED CRYPTOGRAPHY, PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, John Wiley & Sons, Inc., 2d ed., 1996. Many other forms of securing

15   communication are readily apparent to those of skilled in the art.

Data Storage Devices / Memory

For each computer and/or device (i.e., the central computer, the user

20   computer, and/or the monitoring apparatus), a processor may be in communication with a memory and a communications port (e.g., for communicating with one or more other computers or devices). The memory may comprise an appropriate combination of magnetic, optical and/or semiconductor memory, and may include, for example, Random Access Memory (RAM), Read-Only Memory (ROM), a

25   compact disc and/or a hard disk. The memory may comprise or include any type of computer-readable medium. The processor and the memory may each be, for example: (i) located entirely within a single computer or other device; or (ii) connected to each other by a remote communication medium, such as a serial port cable, telephone line or radio frequency transceiver.

30   In one, several or all computers or devices, a memory may store a program for controlling a processor. The processor performs instructions of the program, and thereby operates in accordance with the various methods described in detail

herein. The program may be stored in a compressed, uncompiled and/or encrypted format. The program furthermore includes program elements that may be necessary, such as an operating system, a database management system and "device drivers" for allowing the processor to interface with computer peripheral

5   devices. Appropriate program elements are known to those skilled in the art, and need not be described in detail herein.

The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to a processor for execution. Such a medium may take many forms, including but not limited to, non-volatile

10   media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as memory. Volatile media include dynamic random access memory (DRAM), which typically constitutes the main memory. Transmission media include coaxial cables, copper wire and fiber optics, including the wires that comprise a system bus coupled to the processor.

15   Transmission media may carry acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium

20   with patterns of holes, a RAM, a PROM, an EPROM, a FLASH-EEPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to a processor for execution. For

25   example, the instructions may initially be stored on a magnetic disk of a remote computer. The remote computer can load the instructions into its memory and send the instructions, e.g., over a telephone line using a modem. A modem local to a particular computer or device can receive the data, e.g., on the telephone line, and use an infrared transmitter to convert the data to an infrared signal. An infrared

30   detector can receive the data carried in the infrared signal and place the data on a system bus for the processor. The system bus carries the data to main memory, from which the processor retrieves and executes the instructions. The instructions

received by main memory may optionally be stored in memory either before or after execution by the processor. In addition, instructions may be received via a communication port as electrical, electromagnetic or optical signals, which are exemplary forms of carrier waves that carry data streams representing various

5   types of information. Thus, a computer or device may obtain instructions in the form of a carrier wave.

According to an embodiment of the present invention, the instructions of the program may be read into a main memory from another computer-readable medium, such from a ROM. The execution of sequences of the instructions in a

10   program causes the processor perform the process steps described herein. In alternate embodiments, hard-wired circuitry may be used in place of, or in combination with, software instructions for implementation of the processes described herein. Thus, embodiments of the present invention are not limited to any particular combinations of hardware and software.

15   In one embodiment the memory also stores a plurality of databases, including (1) a site database, and (2) a Guardian database. Some or all of the data stored in each database is described in conjunction with the following description of the process steps. The described entries of the databases represent exemplary information only; those skilled in the art will understand that the number and

20   content of the entries can be different from those illustrated herein. Further, despite any description of the databases as tabular or relational databases, it is apparent that many other methodologies for stopring and retrieving data may be employed. For example, an object-based model could be used to store and manipulate the data types described herein and likewise, object methods or

25   behaviors can be used to implement the processes described herein.

Site Registration

Site owners and/or operators such as owners of nuclear facilities, chemical

30   plants, and airports may be required to initially register with the system in order have their sites monitored by Guardians. It is contemplated that site owners will purchase camera and/or other monitoring device equipment from the operator of

the central computer, although it is possible that site owners may register other existing cameras and/or other monitoring devices with the central computer. In some embodiments, the cameras distributed to site owners are mounted atop poles that can be easily erected in the ground.

5   In embodiments where monitoring devices comprise cameras such as video cameras, cameras and supporting peripheral hardware may have embedded computer devices and may support various standard internetworking and operating system protocols (e.g. embedded Linux chips that support HTTP, SSL, FTP, CGI, Java, etc.). For example, cameras available from Axis® Communications, Inc.

10   may be employed, including model 2420 series network cameras with infrared (IR) lenses, model 250-S MPEG-2 network video servers, and model 2191 audio modules. Infrared lenses may be desirable for low-light (i.e. nighttime) image capture.

        In some embodiments, cameras may also be equipped with PTZ

15   (Pan/Tilt/Zoom) mechanisms to facilitate remote adjustment of field of view, focus, and the like. Further, in some embodiments, cameras may be configured to support on-demand requests (e.g., from the central controller, from site owners, from supervisors) for static and motion images.

        It may also be desirable that cameras are weather-insulated as they may be

20   located outdoors and subjected to extreme temperatures, wind and precipitation. Further, each camera may have two independent circuits, so that if one fails the other can serve as a backup. Similarly, cameras may employ dual, redundant power sources, such that if one power source is unavailable, a back-up power source (e.g. batteries, generators, etc.) may be used. Indeed, in some

25   embodiments, completely autonomous, free-standing image capture hardware may be employed. Such hardware may use solar panels and high capacity energy cells for power, and may use cellular/satellite communications for networking. Such autonomous camera hardware could be used in isolated areas such as deserts and national parks where A/C power is burdensome to obtain.

30   After the site owners obtain suitable monitoring devices, site owners may be required to register with the system by interacting with the central computer in

accordance with the following process steps, which are described as steps performed by the central computer.

Step 1: Receive request to register at least one monitoring device.

5   The central computer receives a request to register at least one monitoring device. The request can be received by the central computer's input device or communication port. Such a communications port or input device may be enabled to receive Dual-Tone Multi-Frequency (DTMF) tones in an Interactive Voice

10   Response (IVR) application. In such an embodiment, site owners would call the central computer via phone, and navigate through an audio menu to complete the registration process. Alternatively, a communications port or input device may be enabled to receive registration commands, via the Internet or other public network, from a computer or monitoring device operated by the site owner.

15   In a further alternate embodiment, cameras may be equipped with USB or other ports so that registration can take place automatically (i.e. "plug and play") upon the establishment of a connection between the camera's port and the central computer.

20   *Step 2: Confirm communication with monitoring device.*

The central computer then sends a test signal (i.e. a "ping") to the monitoring device to confirm its presence and functional ability and, in some embodiments, determine its configuration, location, and other important

25   information.

Step 3: Assign monitoring device identifier and record identifier in site database.

30   Once communication with the monitoring device is established, the central computer then assigns a unique identifier to the monitoring device and records the

12

identifier in a record of the site database, such as that which is depicted in Table 1, herein.

Step 4: Initiate test procedures.

5

In some embodiments, test procedures may be instituted to confirm the monitoring device's ability to detect (i.e. to capture images) as intended. For example, the site owner may be instructed by a supervisor, via a two-way audio communication channel, to adjust a camera so as to enable the widest possible field

10 of view, or to reposition a camera angle to eliminate public areas that cannot be considered no-man zones.

Step 5: Receive and record site-specific rules in site database.

15 In some embodiments, site owners may be prompted to select or otherwise indicate site-specific rules for monitoring. Further, in some embodiments, site owners may be charged premiums for certain levels of service. For example, site owners desiring more or higher levels of security may request lower thresholds or triggers for supervisory review of images. Or, for example, site owners may desire

20 to have at least two "5 star" rated Guardians assigned to monitor images from their site at all times. Such site-specific rules may be recorded in the record corresponding to the assigned monitoring device identifier in the site database, such as that which is illustrated by way of example in Table 1 below. Likewise, custom or standard emergency procedures may be similarly identified and recorded

25 for future reference by the system, its operators or Guardians.

In yet other embodiments, site owners and/or monitoring devices may be prompted to capture reference images for later comparison by the monitoring device and/or the central computer against subsequently captured images.

30

TABLE 1: Site Database

Monitoring device identifier(s)	Site	Contact information	Monitoring rules	Emergency procedures	Billing information
1234-56789 1234-56790 1234-56791 1234-56792	Smith Memorial Airport, Town, Ohio, USA	Bob Johnson, Security Officer, cellular phone number (212) 555-1212	Guardians must be located at least 50 miles from site Guardians must be rated 3 or higher	First, confirm emergency with at least 5 other randomly recruited Guardians. Then, contact Bob Johnson directly via automated outbound IVR call to listed cell phone number. Then, contact local police at (212) 555-	$1000 per month, billed monthly from Bank Account Number 654987987645

				9999	
3333-92931 3333-92932 3333-02033	City Hydraulic Company, City, Texas	Nancy Simmons, Water Purity Specialist, pager number (888) 222-2222	Guardians must always be assigned completely randomly.

Guardians should never receive image from this camera twice. | If security threat is detected by at least two Guardians, request supervisor review of subject image. | $1200 per month, billed monthly from Bank Account Number 5879462865832 |

5   Guardian Registration

In one embodiment, Guardians register with the central computer in order to participate in monitoring sessions and thereby earn compensation for such participation. Registration may take place in accordance with the following

10   process.

Step 1: Receive registration request from potential Guardian.

A potential Guardian transmits to the central computer, via a user device such as a personal computer, cell phone or kiosk, a request to register as a

15   Guardian. For example, a potential Guardian may log on to a website associated

with the central computer and click on a hyperlink to indicate the potential Guardian's desire to register.

Step 2: Prompt potential Guardian for required information.

5   The central computer may then retrieve from memory a list, a "fillable" form, an IVR menu, or other data structure prompting the potential Guardian to input certain required information. The information required may include unique identification data such as a Social Security Number (SSN), a driver's license number, a financial account identifier (credit card account number, debit/checking

10   account number, PayPal® account identifier, etc.), a biometric identifier (e.g. fingerprint), or the like. Further, in order to proceed, the Guardian may be required to answer certain questions, take an oath, agree to the terms of a contract, or otherwise provide assurance that access to the system will not be used for other than its intended purpose. Any or all of such information may be recorded in the

15   Guardian database or elsewhere for future reference.

At this point, based in part on the received information, the central computer may, in some embodiments, initiate a subroutine designed to institute a "background check" of the potential Guardian. Such a subroutine may involve a confirmation of the existence of certain information in remote databases, directly

20   or indirectly accessible to the central computer via a communications port. For example, if a driver's license number is required, the central computer may output a request to a computer operated by a state's licensing authority (e.g. the Connecticut Department of Motor Vehicles) to confirm the validity of the driver's license (i.e. that the license was validly issued and that the name matches that of

25   the potential Guardian). If the results of a background check subroutine indicate that inaccurate or incomplete information was submitted by the potential Guardian, the process may terminate at this point. Otherwise, it may continue.

Step 3: Output instructional data.

30   The central computer may then retrieve from memory and output to the potential Guardian's user device instructional data for the purpose of educating the Guardian about how to participate in monitoring sessions. Such data may take the

form of (1) text, (2) audio, (3) video, or (4) any combination thereof. The content of such data may include, for example, instructions about how to respond to images and questions about images.

5   *Step 4: Initiate testing subroutine.*

        The central computer may then, in conjunction with user device, proceed to initiate a testing subroutine for the purpose of ensuring that the potential Guardian (1) witnessed and understood the instructional data, and/or (2) can perform with a

10   certain minimum level of competency in a test ("mock" and/or "live") Guardian session.

        In embodiments where the testing subroutine is designed to confirm the potential Guardian's comprehension of instructional data, questions may be retrieved from memory and output to the potential Guardian, who would in turn

15   indicate answer choice selections to the central computer via the user device. The central computer could then compare the received answer selections to a stored set of correct answer choices, determine a score, and compare the score to a stored rule indicating a certain minimum required score. If the potential Guardian's score meets or exceeds the minimum required score, the process may continue.

20   Otherwise, it may end or return to any earlier point (e.g. with the output of instructions).

        In embodiments where the testing subroutine is designed to determine whether or not the potential Guardian can perform in a "mock" Guardian session with a minimum required level of competency, the central computer can retrieve

25   and output a stored sequence of test images and questions. The test subroutine would thus determine if, for example, the Guardian can spot humans in no-man zones. Alternatively, a competency test may wholly or partially include "live" images received in substantially real-time from a remote monitoring device. In any event, the potential Guardian's responses are evaluated to determine their accuracy

30   and/or conformance to a central tendency (e.g. mean, median, mode, etc.) of a plurality of responses (e.g. from other Guardians or potential Guardians). If the potential Guardian has performed in accordance with a minimum required level of

competency, the process may continue. Otherwise, it may end or return at an earlier point (e.g. with the output of instructions or with the initiation of another testing subroutine).

It should be noted that the instructional subroutine of Step 3 and the testing
5   subroutine of Step 4 may be combined to form an interactive training session.

Step 5: Create record for Guardian in Guardian database.

The central computer then creates a record for the potential Guardian in a
10   Guardian database, such as that which is depicted herein in Table 2. In creating such a record, the central computer may generate, assign and record a unique Guardian identifier to the Guardian that may be used to track a given Guardian's participation in monitoring sessions so that records can be kept for rating and compensation purposes. Information that was received from the potential
15   Guardian in Step 1 may be recorded in this Guardian database (e.g. SSN, driver's license number, financial account identifier, biometric identifier). The central computer may also request, receive and record other information from the Guardian that may be useful for future tracking, identification, security, compensation, regulatory compliance and/or tax (e.g. withholding) purposes.
20

TABLE 2: Guardian Database

Guardian identifier	*Current Guardian rating (1-5)*	*Guardian identification information*	*Guardian financial account identifier*	*Time Logged this Pay Period*
ABCDEFG	5	Bob Schneider 2 Main Street Town, USA State Driver's Lic # 9999999 SSN 999-99-	Visa® Check Card 8888-8888-8888-8888, Exp 5/07	18 hours, 29 minutes

		9999		
ABNGUYC	4	Tom Meyer 32 Park Avenue City, USA State Driver's Lic # 7K1945 SSN 333-33-3333	Checking Account Number with ABA Routing Code: 706001 1220012 4563271	3 hours, 15 minutes
MGNWOIQ	Temporarily banned from system until retraining completed	Mary Sullivan 913 Broadway Village, USA State Driver's Lic # MS1902 SSN 222-22-2222	PayPal® Account Number 12536	47 minutes

Step 6: Enable download of Guardian software to user device.

After a potential Guardian has achieved the status of "Guardian" by passing all instituted security and competency checks and receiving a Guardian identifier, the central computer enables the Guardian's user device to download any appropriate software necessary to participate in monitoring sessions. In some embodiments, any required cryptographic keys may be downloaded to the user's device. Techniques and protocols enabling the downloading of software applications is well-known to those in the art and need not be described in detail herein.

EXAMPLE

The owners of a nuclear power plant, a privately-owned water reservoir, and an airport each register with the operator of the disclosed system (in this

5   example, named "U.S. HomeGuard") by (a) purchasing cameras, (b) installing them at certain "no-man" zones on the sites' grounds, and (c) participating in an initialization sequence whereby the installed cameras receive Internet Protocol (IP) addresses and capture "reference" images that the system subsequently can use in determining whether to transmit a given image to Guardians.

10   Independently, U.S. HomeGuard recruits a plurality of Guardians to monitor select still images of the no-man zones and report potential security breaches. Guardians may register with the U.S. HomeGuard system by (a) logging on to a central website, (b) providing certain required background information, (c) downloading operational software, and/or (d) receiving identification information

15   such as unique alphanumeric user identifiers.

After registration, Guardians may log on to the U.S. HomeGuard site at any time and participate in the remote monitoring of select no-man zone images captured by the cameras. So as to reduce the number of transmitted images to only potential security breaches, the central computer or the cameras themselves may be

20   configured to only transmit images to Guardians if there is a triggering activity, such as the triggering of a motion detector circuit and/or the determination that a given image does not match stored reference images.

Once captured, images may be routed to Guardians according to stored rules. Such rules may require, for example, that images are (i) transmitted to a

25   threshold number of Guardians (e.g. at least three Guardians), (ii) assigned randomly to Guardians, (iii) routed according to geographical rules (e.g. that Guardians must be physically situated at least 250 miles from the given no-man zone), (iv) assigned to Guardians based on Guardian ratings (e.g. at least one top rated Guardian receives the image), and/or (v) any combination thereof. Such

30   rules would function to enhance the quality of the monitoring service by allowing for redundancy (i.e. by requiring multiple viewers). Such rules would also function to bolster the security of the system by making the routing of feeds

unpredictable (i.e. based on randomness) and/or by maintaining site anonymity (i.e. by routing images based on geographical rules). Many other rules may be implemented consistent with the embodiments of the present invention.

5   Once the Guardians receive images, they are prompted by a user device to indicate if they (1) see a person/vehicle in the picture, (2) do not see a person/vehicle in the picture, or (3) are not sure. The U.S. HomeGuard central computer may maintain a stored set of rules for determining whether a threshold number of responses are received that indicate a potential security threat. If a potential security threat is reported, the central computer may initiate emergency
10   procedures, including verification of the emergency by other Guardians and/or trained professionals, and/or the dispatch of local emergency responders to the site.

      The attentiveness of the Guardians can be tested so as to ensure quality of the monitoring service. For example, a data storage device accessible by the central computer may route to Guardians previously-recorded images that depict
15   real or fabricated security breaches in order to determine whether or not Guardians are paying attention to the routed images. Should Guardians fail to report such "false positives" by indicating the correct response, the central computer may (1) adjust a rating associated with the Guardian, (2) adjust the compensation due to the Guardian, and/or (3) temporarily or permanently disable the Guardian from
20   participating in the system.

      After viewing images, Guardians may log off at will, and may be compensated for their work. Compensation may be determined based on, for example, (i) the amount of time spent monitoring, and/or (ii) the degree of a given Guardian's responsiveness to real or fabricated security breaches. Compensation
25   may take the form of, for example, a credit to a financial account associated with the Guardian, such as a credit card account, a debit card/checking account, or a service account (e.g. an account for services rendered by an Internet Service Provider).

30

Monitoring Sessions

Registered Guardians can initiate monitoring sessions at any time. That is, they need not have previously scheduled a monitoring session.

5

Step 1: Receive request to initiate session.

Monitoring sessions begin when a Guardian sends a request to the central computer to initiate a monitoring session. In some embodiments, various security
10   protocols are employed to verify the potential Guardian, such as by ensuring that only registered Guardians participate in monitoring sessions. For example, Guardians may be required to submit their Guardian identifiers that were distributed during the Guardian registration process. Guardian identifiers may be submitted without active involvement on the Guardian's behalf, for example, as
15   may happen if the Guardian's user device stored a "cookie" file, accessible to the central computer, that contained the Guardian's identifier. Further, Guardians may be required to submit verifiable passwords in a manner known in the art. Indeed, any level of security desirable and known in the art may be employed.

At this point, a subroutine may optionally be employed to verify the
20   coordination and attentiveness of the Guardian. For example, the central controller may administer, in conjunction with the Guardian's user device, a simple test of the user's coordination (e.g. by requiring the user to trace a line with the mouse cursor) or of the user's reaction time (e.g. by requiring the user to depress the Enter key immediately after seeing an image of a human). Such a test may be useful in
25   determining whether or not the Guardian is currently in an appropriate (i.e. sober, rested) state to participate in a monitoring session.

Alternatively or additionally, the central computer may employ yet another subroutine to determine if the Guardian is temporarily or permanently banned from the system. More specifically, the central controller may use the submitted
30   Guardian identifier to retrieve Guardian rating information from the Guardian database and determine whether or not the Guardian is temporarily or permanently banned from the system. For example, referring to the third exemplary record in

Table 2, Mary Sullivan may be banned from the system until she successfully completes a retraining routine similar or identical to that which is disclosed in Steps 3 and 4 of the Guardian registration process. Should a Guardian be temporarily or permanently banned from participating in monitoring sessions, the

5   central computer may direct the Guardian to participate in retraining or may end the process, as appropriate.

Step 2: Identify captured data (i.e. image).

10   Previously, substantially simultaneously, or subsequently, the central controller may identify an image (or other data) that is available for Guardian review.

In some embodiments, monitoring devices such as cameras may have previously or substantially simultaneously captured images or other data and

15   transmitted such data to the central computer. Monitoring devices may be configured to automatically capture and transmit such data upon the happening of a "triggering" or "image capturing" event, such as (1) the initiating of a motion detector circuit, (2) the detection of thermal changes in a camera's field of view, and/or (3) the detection of a mismatch between a captured image and a previously

20   stored reference image.

In an alternate embodiment, an acoustic perimeter intrusion detection (APID) system may be used to trigger the capture of images. APID systems, such that which is manufactured by ESCI International, Inc. of Clifton, New Jersey, include one or more metal wires attached to physical ballast dampeners operatively

25   connected to a computer. The wires are attached on or adjacent to a physical fence, and the computer monitors the wires for acoustic vibrations. If vibrations are detected, the computer locates the exact position of the intrusion by monitoring the vibrations on the fence and determining the time that the signals are received from several locations. Such a detected intrusion may in turn trigger the capture

30   and routing of images in the inventive system.

In some embodiments, when an image capture event occurs, the camera hardware may post one (or more) images to the central computer and may also

isolate and index a full-motion image buffer (of configurable duration before and after the triggering event) and preserve this buffer in local or remote storage for a finite time period (e.g., 48 hours).

Also, in some embodiments, the central computer may queue the captured

5   image(s) in a routing database, from which images are retrieved and routed to Guardians as described in the following step.

Step 3: Route data to at least one Guardian.

10   After the central computer identifies the data, the data is routed to at least one currently active Guardian for review. In some embodiments, the central computer may route the data to Guardians randomly, based on stored rules, or a combination of both. As disclosed herein, stored rules may be site-specific rules selected by the site owner (see, e.g., columns 4 and 5 of Table 1.).

15   Alternatively or additionally, the central computer may be configured to impose certain routing rules to ensure quality and security, as discussed herein. For example, the system may require a minimum level of Guardian redundancy. That is, the central computer may require that a minimum number of Guardians review a given image. Further, the central computer may dynamically (i.e.

20   periodically or continuously) adjust such rules for any or all sites based on (1) the number and quality of available Guardians at any point in time, and/or (2) a "threat level" obtained from a remote database, such as one maintained by the United States Department of Homeland Security.

In some embodiments, the routing of captured images includes the routing

25   of response instructions and/or possible answer selections. For example, Guardians could be prompted to indicate if they (1) see a person in the picture, (2) do not see a person in the picture, or (3) are not sure. Alternatively, Guardians could be presented with two images (i.e. one prerecorded reference image and one subsequently captured image) and asked whether or not the two images are a

30   match.

Additionally or alternatively, the central controller may at this step retrieve a false image from a database and transmit the false image to at least one Guardian.

The central controller may be configured to transmit false images (1) randomly, and/or (2) periodically, based on stored rules (e.g. every X images, every Y minutes).

5   *Step 4: Identify response(s).*

Guardian responses are then transmitted to and received by the central computer. In some embodiments, if an image is presented to a Guardian and a response is not subsequently received by the central computer within a given time

10   interval, the image "response instance" is redistributed to another Guardian meeting the routing rules for the given image. That is, the image may be transmitted to another Guardian.

In yet other embodiments, if an image is not voted on by the minimum number of Guardians within an overall expiration time interval, the image may be

15   routed to supervisors or otherwise processed in accordance with site-specific rules.

Step 5: Evaluate received response(s) and process accordingly.

If responses indicating a potential security breach exceed a site-specific

20   threshold (e.g. 2 out of 3 Guardians indicate that there is a human in a no-man zone), certain procedures may be implemented depending on site-specific or general system rules. For example, if a threshold number of Guardians report a human in a no-man zone, the subject image can be routed to one or more Guardians for confirmation (e.g. Guardians with higher ratings), routed to one or

25   more supervisors for confirmation, and/or routed to the site owner for confirmation.

Similarly, if an image is not voted on by a required minimum number of Guardians within an overall expiration time interval (site/node configurable) the image may be escalated according to rules (e.g., rules specific to the site).

30   Similarly, if an image if presented to a Guardian and is not subsequently voted on within a time interval, then that Guardian's vote can be invalidated and the image "vote instance" is redistributed. The time interval may be site/node

configurable. Guardian votes are posted and processed by a vote management service.

If affirmative votes exceed a site/node defined threshold then the image may be "escalated" according to site rules. Site escalation rules may dictate, e.g.,

5   that any of the following occur during image escalation:

(a) Image goes through a second wave of distribution to Guardians based on routing logic defined for that escalation level (e.g. to Guardians with higher average accuracy scores).

(b) All image capture nodes for escalated site immediately register capture

10   events, post images for review, and cache full-motion buffers regardless of motion detection status.

(c) Image capture nodes that provided the original image(s) undergoing escalation will be instructed to upload the motion image buffer(s) associated with the original image to the image services network which will make these buffered

15   images available to Supervisors as needed.

When an appropriate escalation level is reached, a site alert may be created and posted to a site incident portfolio for Supervisor review.

Image routing and escalation rules may ultimately be driven be an AI/Bio network and/or a cognitive rules engine of some kind (though initially will be

20   driven by a meta-data rule base — the prototype uses logic coded in database stored procedures and tables).

Alternatively or additionally, should a potential security breach be detected, the central computer may enable a two-way audio and/or video communication channel to the corresponding site so that a supervisor can talk to any person in the

25   camera's proximity. In such an embodiment, the supervisor would have the ability to initiate a challenge/response (or "stand down") procedure by asking the person questions that may indicate their authority to occupy the given space (e.g. passwords).

In yet another alternate embodiment, should a potential security breach be

30   detected, the central computer may dispatch local emergency responders, contact the site owner and/or notify another entity. The central computer may further route any relevant captured images to the emergency responders and/or site owner via,

for example, a high-bandwidth handheld device such as a 3G enabled cellular telephone. Further, the central computer may activate: (a) an electric fence, (b) an alarm, and/or (c) other site-specific devices and procedures.

Further, site-specific rules may dictate that any or all of the following occur

5   in the event of a potential security breach: (1) all cameras corresponding to the relevant site may immediately capture images, post images for review, and cache full-motion buffers regardless of motion detection status; (2) the cameras that provided the original image(s) may be instructed to upload the motion image buffer(s) associated with the original image to the central computer, which will

10   make these buffered images available to supervisors and/or emergency responders as needed; and (3) a site alert may be created and posted to a site incident portfolio for Supervisor review.

In embodiments where the central controller transmitted at least one false image to at least one Guardian, the relevant Guardian's response may be evaluated.

15   The system may compare the Guardian's response against a stored set of correct or preferred answers, and inaccurate or undesirable responses may lead to negatively adjusted ratings, as discussed with reference to the next step.

      Step 6: Adjust Guardian rating based on evaluation of received
20   *response(s).*

As discussed herein, Guardians can be categorized according to their current skill level (determined by their performance in evaluating real and false images). In some embodiments, Guardians in good standing may be given a

25   numerical score and Guardians who are temporarily or permanently banned from participating in monitoring sessions may be so marked in corresponding database records (see, e.g., Table 2).

According to an alternate rating scheme, a Guardian can be in "good standing", "on probation", "suspended", or "banned". The scoring thresholds that

30   define the category boundaries can be configured at the site level. The rules defining the effect of a status and the requirement for moving out of a status can be defined system-wide and overridden at the site level as necessary. Example rules

include (a) a "good standing" Guardian may receive real (i.e. live) images and test images according to stored image routing rules, (b) a Guardian who is "on probation" may only receive test images until their score moves them back into the "good standing" category (this category might be initially in effect for new

5   Guardians); (c) a Guardian who is "suspended" may need to take a remedial on-line training course and pass it to move into the "on probation" category, (d) a Guardian who is "banned" would not be allowed back on the system.

Step 7: Receive request to terminate at session.

10

At any time, a Guardian may unilaterally end his or her participation in a monitoring session by transmitting to the central server a signal so indicating.

It should be noted that, in an alternate embodiment, the step of adjusting Guardian ratings (Step 6) may take place after the step of receiving a request to

15   terminate the session (Step 7).

Step 8: Calculate and initiate provision of compensation to Guardian.

The central computer system may then determine the amount of

20   compensation due to a Guardian and initiate the provision of compensation. Guardians may be afforded different pay rates according to their rating status. For example Guardians rated at "5" may receive a rate of $8/hour, while Guardians rated at "4" may receive a rate of $7.50/hour. In such an embodiment, the central computer would multiply the amount of time logged by the Guardian by the given

25   Guardian's pay rate. This could be done after each Guardian session, or, alternatively, could be done periodically (e.g. weekly, monthly) or upon the Guardian's request.

The central controller may initiate payment by instructing that an account associated with the Guardian be credited. Methods for crediting accounts and

30   transferring funds are well known and need not be described in detail herein.

Alternate payment mediums are contemplated, as discussed herein with reference to the section entitled "Additional and Alternate Embodiments".

Additional Embodiments

In some embodiments, the probability of a Guardian receiving a test image instead of a live image may be driven by a calculation that increases the probability
5   in inverse proportion to their current accuracy rating.

In some embodiments, test images may be categorized for degree of difficulty and this degree of difficulty may "weight" a Guardians score when they submit responses associated with these images.

In some embodiments, test images may be categorized by visual
10   characteristics (e.g. snow, water effects, low light, wide angle) and a scoring engine may be used to increase the probability of a Guardian scoring well in that category getting a site image that matches these characteristics.

In some embodiments, image routing and escalation rules may ultimately be driven be an artificial intelligence network and/or a cognitive rules engine.
15   In some embodiments, Guardians who have previously reviewed images for a particular site can be assigned a higher or lower probability of reviewing an image from the same site (or they may be excluded completely).

In some embodiments, test images may be given accompanying "answer" images that highlight the part of the image that contains a person (for false
20   positives) or explain that there is no person (for false negatives) and this "answer" image may be presented to the Guardian immediately after erroneously voting on the test image.

In yet another alternate embodiment, site anonymity can be further maintained by employing stored rules that function to actively suppress the
25   transmission of location-specific information from the Guardians. For example, using artificial intelligence, the system may pre-screen all images and redact any text therein (e.g. signage), so that information relevant to the site's location is not transmitted to the Guardians.

In some embodiments, supervisors may access the system via a supervisor
30   interface that may be a highly secure internet-accessible (e.g. SSL browser w/ RSA authenticated VPN connection) tool used to manage, prioritize and resolve site alerts.

In some embodiments, the supervisor interface can enable the supervisor to adjust PTZ orientation of any camera, and can enable the supervisor to engage in two-way audio communication via appropriately configured image capture nodes.

In some embodiments, supervisors can schedule planned maintenance

5   outages for monitoring devices.

In some embodiments, the supervisor interface may present all captured images related to a site incident file. These images will be provided in both full resolution and thumbnail for quick reference.

In some embodiments, the supervisor interface can enable Supervisors to

10   access and review the full motion image buffers surrounding alert images from all sites and monitoring devices.

In some embodiments, the supervisor interface can enable supervisors to access real-time full motion images from any monitoring device.

In some embodiments, supervisors can adjust motion sensor zones and

15   sensitivity for monitoring devices.

In some embodiments, when Guardians and Supervisors register with the system they will be asked to record a number of confidential question/answer pairs related to their personal information. In addition to secure site password login, these questions will intermittently be posed to Guardians/Supervisors when they

20   log in as a means of supplemental authentication. The requirement for and frequency of this authentication can be configured at the site level for Supervisors and can be driven by score and/or status for Guardians.

In some embodiments, supervisor authentication security may be supplemented by a hardware-based key generation device (e.g. RSA key fob).

25   In some embodiments, multiple redundant core data centers may be employed.

In some embodiments, all Guardian access may be via authenticated SSL browser connections.

In some embodiments, a "single sign-on" rule will be enforced for

30   Guardians so that Guardians cannot participate in two monitoring sessions simultaneously.

In some embodiments, anti-fraud check logic may be used to prevent re-establishment of banned Guardians (personal and financial data matching algorithms, network usage patterns, etc.).

In some embodiments, administrators will access the supervisor interface
5   via a browser through secure network tunnels (e.g. authenticated VPN connections).

In some embodiments, Guardian compensation levels may be adjusted by local hour of the day to promote participation during periods of low Guardian on-line activity (e.g. 1-5 AM EST).

10   In some embodiments, Guardians may be compensated in the form of tax credits. For example, Guardians may be offered an alternative way to pay their federal income taxes by participating in the system. In such an embodiment, Guardian SSNs will be used to track such earned tax credits.

Similarly, prisoners may be afforded the opportunity to earn "good
15   behavior" credit by participating in monitoring sessions.

In some embodiments, Guardians may be compensated by being offered the chance to win a sweepstakes prize. In such embodiments, a game may be incorporated into the monitoring session program. For example, Guardians who view and report winning game pieces in images may receive a prize. Such
20   sweepstakes would encourage attentiveness and provide a different form of economic motivation.

Further, Guardians may be rewarded with bonuses or enhanced compensation for spotting real emergencies.

In some embodiments, all remote monitoring devices will receive a
25   "heartbeat ping" (i.e. a query) issued by the central computer at a configurable interval. Devices that do not respond may immediately trigger the initiation of emergency procedures.

In some embodiments, at an interval defined at the site level, the monitoring devices will be instructed to post a static image regardless of motion
30   detection status. This image can be analyzed by the image processing network and compared to the last image from the same device to determine if significant composition change has occurred that would imply movement and, if so, route the

image for Guardian review. The sensitivity of this analysis can be site or device specific.

Rather than physical property, Guardians could monitor complicated computer systems, and the monitoring device could be some type of software

5   analysis of network patterns, rather than a camera. For example, no accesses of a certain type should be made, and the system can graphically represent such accesses for ease of analysis by Guardians. This type of monitoring could be done by Guardians who possess certain basic computer skills.

Similarly, the system could be configured to monitor sounds. Relatively

10   unskilled Guardians could distinguish mundane sounds from, e.g., shouting, cries for help or gunshots. In one embodiment, sound monitoring (which is very low bandwidth) could be used in conjunction with image monitoring to direct images of certain sites to more Guardians. This works especially well even in sites which are not strictly 'no-man' zones.

15   In some embodiments, cameras may be mobile or mounted on mobile vehicles (cars, trucks, unmanned flying drones, etc.) to enable monitoring of a plurality of sites. Again, sites need not be no-man zones. For example, cameras may be mounted on a patrol vehicle, and Guardians could monitor an area much better while the driver conducts a foot patrol.

20   In some embodiments, a subset of monitoring devices may be randomly or otherwise activated/deactivated at a given time based on the number and/or quality of available Guardians. Such an embodiment would function to increase the level of security at times when there are more cameras than active/qualified Guardians.

In some embodiments, site owners may be charged based on the number of

25   images actually reviewed by Guardians in a given amount of time.

In some embodiments, cameras configured at highly or densely populated areas (ATMs, toll booths, shopping malls, etc.) and Guardians may actually be asked to compare still images of human subjects captured from such cameras against a reference image of a particular human in order to determine if there is a

30   "match". For example, Guardians could log on and compare, one by one, the many captured images taken from the millions of security cameras nationwide against a given picture of a fugitive or a missing person. Guardians could simply

indicate "match" or "no match". Thus, the abundance of captured images that may contain the fugitive or missing person could be viewed by Guardians in hopes that fugitives could be caught and missing persons located. In the rare event that a match is detected, the date, time and position of the image-capturing camera can be

5   used to reconstruct the subject's trail and isolate the subject's whereabouts.

       The following examples illustrate various embodiments of the invention which may be advantageously employed to achieve various utilities.

10   The site supervisor module will execute any appropriate automated alert notification processes defined for the site (e.g. page, email, cell notification w/ image).

       Supervisors can "stand down" image escalation at any level and close out site alerts and site incident portfolios.

15   The system will archive/purge static and motion images associated with closed alerts in accordance with site-defined rules.

       Raw images posted from image capture nodes will be optimized for Guardian review through an image processing service that will do things such as grayscale the image, enhance brightness & sharpness, etc. The pre-processing

20   software can be configured at the site/node level to tune it to the visual characteristics of a particular node (e.g. heavy sun glare at certain hours). The "raw' (pre-processing) image may be retained for a site-defined time period and is then discarded.

       All processed images are given a unique index number that associates them

25   with the source site/node.

       After being processed, images are posted to a content distribution network to facilitate image fetch load distribution.

       Guardians who have previously reviewed images for a particular site/node can be given higher or lower probability of reviewing an image from the same

30   site/node (or they may be excluded completely).

       Test images have accompanying "answer" images that highlight the part of the image that contains a person (for false positives) or explain that there is no

person (for false negatives) and this "answer" image is presented to the Guardian immediately after erroneously voting on the test image (before any available live images are presented).

5   The probability of a Guardian receiving a test image instead of a live image may be driven by a calculation that increases the probability in inverse proportion to their current accuracy rating.

Test images may be categorized for degree of difficulty and this degree of difficulty may "weight" a Guardians score when they vote on these images.

Test images may be categorized by visual characteristics (e.g. snow, water
10   effects, low light, wide angel) and a scoring engine may be used to increase the probability of a Guardian that scores well in that category getting a site image that matches these characteristics.

Guardians can be categorized according to their current skill level
15   (determined by their performance in evaluating seeded test images). A Guardian can be in "good standing", "on probation", "suspended", and "banned". The scoring thresholds that define the category boundaries can be configured at the site level.

The rules defining the effect of a status and the requirement for moving out
20   of a status can be defined system-wide and overridden at the site level as necessary. Example rules might be:

A "good standing" guardian receives live images and test images according to the image routing logic engine's determination.

A Guardian who is "on probation" only receives test images until their
25   score moves them back into the "good standing" category. This category might be initially in effect for new Guardians.

A Guardian who is "suspended" would need to take a remedial on-line training course and pass it to move into the "on probation" category.

A Guardian who is "banned" would not be allowed back on the system.
30   When Guardians and Supervisors are set up on the system they will be asked to record a number of confidential question/answer pairs related to their personal information. In addition to secure site password login, these questions

will intermittently be posed to Guardians/Supervisors when they log in as a means of supplemental authentication. The requirement for and frequency of this authentication can be configured at the site level for Supervisors and can be driven by score and/or status for Guardians.

5   Supervisor authentication security may be supplemented by a hardware-based key generation device (e.g. RSA key fob).

Guardian compensation levels may also be adjusted by local hour of the day to promote participation during periods of low Guardian on-line activity (e.g. 1-5 AM EST).

10   The site supervisor interface is a highly secure internet-accessible (e.g. SSL browser w/ RSA authenticated VPN connection) tool used to manage, prioritize and resolve site alerts.

The interface presents all image capture node images related to a site incident profile. These images will be provided in full resolution and thumbnail
15   for quick reference.

The interface can enable Supervisors to access and review the full motion image buffers surrounding alert images from all site image capture nodes.

The interface can enable supervisors to access real-time full motion images from any site image capture node.

20   The interface can enable the supervisor to adjust PTZ orientation of any node camera, and can enable the Supervisor to engage in two-way audio communication via appropriately configured image capture nodes.

Supervisors can schedule planned maintenance outages for nodes and establish ongoing hours of operation for nodes.

25   Supervisors can adjust motion sensor zones and sensitivity for image capture nodes.

Driving parameters for escalation rules are maintained by the site supervisors through this interface (e.g. votes needed for escalation, escalation path, etc.).

30   Alert data and images may be dispatched from the supervisor interface to remote parties via electronic means (e.g. cell phone, email, etc).

Granular role-based permissions can be enforced on all site supervisor functionality.

Camera and supporting peripheral hardware used in image capture nodes will have embedded computer devices and will support various standard

5   internetworking and operating system protocols (e.g. embedded Linux chips that support HTTP, SSL, FTP, CGI, Java, etc.).

Axis camera hardware (2420 series network cameras with IR lens, 250-S MPEG-2 network video servers, 2191 audio modules) may be used as image capture devices. This hardware features embedded Linux chips and open protocols

10   as described above. The cameras and peripherals are networked using wireless bridges — the wireless interface would optimally be on-board (as an add-in capability to save cost when not needed).

Camera hardware located outdoors will be housed in protective covering and will be hardened to tolerate temperature extremes.

15   Camera hardware may be equipped with IR lenses for low-light image capture.

Camera hardware may be equipped with PTZ (Pan/Tilt/Zoom) mechanisms to facilitate remote adjustment of field of view, focus, etc.

Image capture node hardware will support on-demand requests for static

20   and motion images submitted by remote services (such as the site administrator module).

It may be possible to implement completely autonomous, free-standing image capture hardware that uses solar panels and high capacity energy cells for power and cellular/satellite communications for node networking. (These could be

25   used in isolated areas such as deserts and national parks).

Image capture node networking may include use of 802.11b and related wireless protocols.

Image capture node networking may include use of cell networks (GSM and other emerging standards).

30   Multiple redundant core data centers will form the backbone of the services layer.

A content distribution network (numerous distributed nodes) will be used for image distribution.

All Guardian access will be via authenticated SSL browser connections.

Single sign-on will be enforced for Guardians.

5   Anti-fraud check logic will be used to prevent re-establishment of banned Guardians (personal & financial data matching algorithms, network usage patterns, etc.).

Administrators will access the supervisor interface via browser through secure network tunnels (e.g. authenticated VPN connections).

10   DOS attacks (e.g. spoofing and flooding of Guardian image votes) will be a significant concern. Anti-spoofing measures will be implemented to disregard forged image requests and vote responses before they are processed by the appropriate services. Examples of these might be network pattern analysis engines that identify and suppress redundant image requests and vote responses.

15   All site image capture notes will receive a heartbeat ping issued by remote management services at a configurable interval. Nodes that do not respond will immediately generate a site alert and incident portfolio and alert will trigger appropriate escalation as defined by the site rule base.

At an interval defined at the site/node level the image capture nodes will be

20   instructed to post a static image regardless of motion detection status. This image can be analyzed by the image processing network and compared to the last image from the same node to determine if significant composition change has occurred that would imply movement and if so process the image for Guardian review. The sensitivity of this analysis can be site/node configurable (if need be all "health"

25   snapshots can be submitted for review).

DEFINITIONS

The following definitions are used herein above, unless otherwise indicated.

30   *Central computer, central controller, central server, server* - A computer or computing device, which typically comprise at least one or more of: (i) a processor, such as one based on the Intel® Pentium® series processor, (ii) a means

for receiving signals from at least one monitoring apparatus, (iii) a means for transmitting signals to at least one user computer, and/or (iv) a data storage device/ memory. For example, the central computer may be one or more IBM E-series™ servers.

5

False positive, false image, fabricated image, fabricated security breach - an indication which, if transmitted to a Guardian, should to elicit a positive response. For example, the false positive may be a pre-recorded image or other data file depicting a real or fictitious site or no-man zone.

10 *Guardian* - A citizen who participates in the remote monitoring of sites, typically in exchange for compensation.

Monitoring apparatus, monitoring device, sensor - A device capable of receiving or generating (e.g., via an input device such as a charge coupled device) a signal

15 indicative of a sensed state (e.g., an image) and data representing the sensed state (e.g., a captured image). A monitoring apparatus may include, e.g., (i) a processor, such as one based on the Intel® Pentium® series processor, and/or (ii) a data storage device/ memory. Such sensors include, but are not limited to: (a) digital video cameras, (b) digital video cameras equipped with motion detection and/or

20 "short loop" tripping features, (c) digital cameras, and (d) motion detectors. A monitoring devices may be capable of converting analog signals into digital data files.

"No-man" zone - An area, usually a security-sensitive area on a site, where no

25 humans or vehicles should be monitored (e.g. no humans should be present). No-man zones may include areas adjacent to, within, outside of or otherwise in proximity to sites such as airports, chemical plants, natural gas plants, pipelines and pumping stations, power plants (including nuclear reactors), refineries, and reservoirs.

30

Site, Remote Site, Property - Property, including but not limited to real property, containing critical infrastructure or other resources which are to be monitored. Such property may be monitored by one or more monitoring apparatus.

5   *Supervisor, Trained Professional, Professional* - A supervisor may assist site owners in configuring and initializing monitoring devices. A supervisor may receive certain images after review by at least one Guardian. A supervisor may be, e.g., an employee or agent of the owner / operator of the central computer.

10   *User computer, user device, device* - A device capable of (i) receiving a signal (e.g., sensed data) from a central computer and/or a monitoring apparatus, e.g., via a standard Internet connection; (ii) outputting a signal to a Guardian or other user, e.g., via a Web browser displayed on a monitor; (iii) receiving a response from a user, e.g., via an input device such as a mouse, keyboard and standard Microsoft

15   Windows® interface, and / or (iv) transmitting a signal indicative of the response (e.g., a result) to a central computer and/or a monitoring apparatus, e.g., via a standard Internet connection. In some embodiments, a user device may include (1) a processor, such as one based on the Intel® Pentium® series processor, and/or (2) a data storage device/ memory. Examples of user devices include appropriately

20   configured personal computers, cellular telephones, and game stations such as the Xbox® and the PlayStation® game stations.

Neuron - a component which is capable of (i) receiving a signal (e.g., sensed data) from a central computer and/or a monitoring apparatus, e.g., via a standard Internet

25   connection; and (ii) transmitting a signal indicative of the result (e.g., based on processing the received signal) to a central computer and/or a monitoring apparatus, e.g., via a standard Internet connection. In some embodiments, a user device may include (1) a processor, such as one based on the Intel® Pentium® series processor, and/or (2) a data storage device/ memory. Examples of user

30   devices include appropriately configured personal computers (e.g., a user computer operated by a Guardian), cellular telephones, and game stations such as the Xbox® and the PlayStation® game stations.

In another embodiment of the invention discussed above, disclosed below are systems and methods facilitating the *ad hoc* performance of tasks by workers. According to some embodiments, a network of devices is configured to enable

5   individual workers to log on to a central system at any time through devices such as personal computers and cellular telephones and perform low-skill tasks. Such workers may terminate work sessions unilaterally and are compensated based on the amount of work performed.

According to some embodiments, the central system is configured to

10   receive and register task information from at least one employing party. Further, according to some embodiments, the central system is configured to register remote workers. Additionally, according to some embodiments, the central system is configured to manage work sessions. Further still, according to some embodiments, the central system is configured to manage the financial settlement

15   of work sessions, including the billing of an employing party, the compensation of workers, and the allocation of commissions to the operator of the central system. Many additional and alternate embodiments are also disclosed.

In this manner, the systems and methods disclosed herein allow, e.g., low-skill workers to supplement their incomes. Further, the systems and methods

20   disclosed herein allow workers of all skill levels to earn income at heretofore unproductive times by remotely performing low-skill tasks in an *ad hoc*, fluid manner. Additionally, by enabling the remote performance of *ad hoc* tasks, the systems and methods disclosed herein allow employers to purchase labor in incremental units that traditionally would not be economically feasible due to

25   travel costs and hourly pay structures.

Examples

Example 1

30   An Internet service provider such as America Online® (AOL) has configured its computer system to receive job requests from remote employers via the Internet. A manufacturing company registers with AOL to have digital images

40

of its assembly line process reviewed for irregularities by AOL subscribers. AOL and the manufacturing company agree that the company will pay $5,000 for every 100,000 images viewed by two independent AOL subscribers. The parties also agree that AOL will compensate subscribers as it sees fit. Accordingly, AOL

5   decides to retain $1000 of every $5000 received from the manufacturing facility, leaving $4000 to compensate the duplicative viewing of 100,000 images (i.e., 200,000 images). Accordingly, AOL will thus pay AOL subscribers to view images at the rate of $.02 per image ($4000/200,000 images = $.02/image). After the job is registered, AOL then actively advertises the opportunity to its

10   subscribers. As advertised, subscribers would log on to AOL and view digital images of products at a particular stage of an assembly line, one after the other. Subscribers are instructed to click the "OK" or "ERROR" buttons on their screen, depending on whether or not the particular images match a given reference image that represents a high-quality, error-free unit at the given point in the assembly

15   line.

       Bill Jones, an AOL subscriber, is a low-wage worker who works a full-time job in a grocery store. One month, Bill is surprised with a $200 unexpected furnace repair bill. Concerned that his current financial resources are insufficient, Bill logs on to AOL with the intent of emailing a relative and asking to borrow

20     $200. However, Bill's attention is drawn to an area on the AOL graphical user interface (GUI) advertising the opportunity to get paid for performing online quality control monitoring. Bill clicks on the advertisement and begins work immediately by comparing the scrolling series of images on the left side of his screen against the "control" or reference image on the right hand side of the screen,

25   entering "OK" if the images match, and "ERROR" if the images are not a match. Over the next few evenings, Bill logs on and reviews a total of 10,000 images and thereby earns $200. Once he reaches his goal, he transmits a request to AOL's server to get paid, and the $200 is immediately credited to his debit/checking account already on file with AOL.

30

Example 2

       A news organization has arranged with Verizon Wireless to pay subscribers

for answering survey questions. Mary Johnson, a Verizon subscriber, is a commercial real estate agent working almost entirely on commission. One evening on her way home from work, while reflecting on the recent slump in sales, she is delayed in an unexpected traffic jam. Her thoughts turn to the rising price of gas,

5   her high mortgage bills, and her son's college tuition. Overwhelmed and frustrated, she decides she must try to make this time productive. However, at 6:00PM, it's too late catch her clients in their offices. But, she does recall seeing Verizon marketing materials offering the opportunity to get paid for answering survey questions. She puts on her earpiece/microphone unit, presses #WORK

10   (#9675) on the keypad of her cellular phone, and starts answering survey questions by listening to the questions, and responding verbally to prompts from an Interactive Voice Response Unit (IVRU).

For example, the IRVU may output the question "Do you support an increase in the federal income tax to fund increased healthcare benefits for senior

15   citizens? Yes or no?" After deliberating for a moment, Mary responds "no", and the IVRU uses voice-recognition technology to interpret, digitize and record her response. Then, the IVRU may ask "Do you think the income tax on stock dividends should be repealed?" Mary would likewise provide her response. After ½ hour of sitting in traffic, Mary has earned $12, more than enough to pick up

20   dinner for herself and her son on the way home.

Example 3

Jennifer, an America Online subscriber, is a teenager who regularly uses AOL's Instant Messenger to communicate with her friends. While instant

25   messaging, Jennifer earns money by answering survey questions from interested commercial entities such as Old Navy, Abercrombie & Fitch, Capital Records, MTV® and the like. Because she is paid per question answered (rather than hourly), it is perfectly acceptable for her focus to change as she crafts instant messages, fields phone calls, changes radio stations, and the like. She can answer

30   questions when it is convenient for her. For example, while waiting for a friend to respond to an Instant Message, she may answer a survey question in a different window of the AOL GUI.

DEFINITIONS

The following definitions are used herein below, unless otherwise indicated.

Ad hoc task, micro-task, micro-work, piecemeal work, piecework, task- A
5   compensable unit of work registered with a central service by an employing party,
the performance of which taking place at any time thereafter by a remote worker.
Generally, *ad hoc* tasks are comprised of finite, incremental units of work that
together form a broader project or objective for the employing party. For example,
a survey may be divisible into many discrete, individually-compensable questions.
10   The division of projects into such micro-tasks facilitates the beginning and ending
of tasks in an *ad hoc,* impromptu manner. For example, because it only takes a
few moments to complete a single survey question, a worker who does not have
much time may quickly log on, complete a question or two, and then log off. In
order to facilitate the impromptu performance of tasks by a wide range of workers
15   during a wide range of times, *ad hoc* tasks are generally low-skill tasks.

Central computer, central controller, central server, server - A computer
comprising at least one or more of: (i) a processor, such as one based on the Intel®
Pentium® series processor, (ii) a means for receiving signals from at least one
20   monitoring apparatus, (iii) a means for transmitting/receiving signals to/from at
least one worker device, and/or (iv) a data storage device/memory. Generally,
central computers are owned, operated and maintained by communications
services such as cable, phone and/or Internet services.

25   *Employer device-* A computer comprising at least one or more of: (i) a processor,
such as one based on the Intel® Pentium® series processor, and/or (ii) a means for
transmitting/receiving signals to/from at least one central computer. In some
embodiments, employer devices are used to upload information regarding low-skill
tasks, including task content and payment terms.
30

Employing party, employer- A party who registers a task with a central operator
and compensates the central operator and/or one or more remote workers for the

performance of the task.

Low-skill task- Low-skill tasks are tasks, jobs, or other units of work that require little or no worker credentials and can be performed by providing a simple
5   communication responsive to a transmission of task information. Generally, low-skill tasks are relatively non-imposing when compared to other, more mentally consuming (i.e. higher skill) tasks. Thus, low-skill tasks generally can be performed by workers while workers are engaged in other activities. Further, low-skill tasks generally can be started and stopped quickly and fluidly, without
10 significant "switching cost".

Monitoring device- A device located at a site associated with an employing party that is configured to communicate with a central computer and/or a worker device so that workers can receive site-specific data and perform tasks based on the site-
15 specific data. For example, a monitoring device may comprise a video camera, and a micro-task may involve viewing an image captured by the video camera and responding as to the contents of the image.

Work session- A period of time during which a remote worker performs at least
20 one micro-task. Generally, work sessions include a plurality of micro-tasks.

Worker- A person who communicates, via a worker device, with a central computer and/or a monitoring device for the purpose of earning compensation in exchange for the performance of micro-tasks. Generally, workers need not possess
25 particular skills, as most micro-tasks are low-skill tasks. Further, workers are often subscribers to a communications service such as a cable, phone and/or Internet service.

Worker device, user computer, user device- A device capable of (i) receiving a
30 signal from a central computer and/or monitoring device, (ii) outputting a signal to a user (i.e. a worker), (iii) receiving a response from a user via an input device, and (iv) transmitting a signal indicative of the response to a central computer and/or

monitoring device. In some embodiments, a user device may include (1) a processor, such as one based on the Intel® Pentium® series or Centrino® series processor, and/or (2) a data storage device/ memory. Example worker devices include personal computers, Personal Digital Assistants (PDAs) and cellular

5   telephones.

Network configuration

10   The embodiments described below can be configured to work in a network environment whereby the central computer, the user computer, the employer device, and/or the monitoring device communicate with each other directly or indirectly, via a wired or wireless medium such as the Internet, LAN, WAN or Ethernet, Token Ring, or via any appropriate communications means or

15   combination of communications means. Communication between the devices and computers, and among the devices, may be direct or indirect, such as over the Internet through a Website maintained by a computer on a remote server or over an on-line data network including commercial on-line service providers, bulletin board systems and the like. In yet other embodiments, the devices may

20   communicate with one another and / or a computer over RF, cable TV, satellite links and the like.

Some, but not all, possible communication networks that may comprise the network or be otherwise part of the system include: a local area network (LAN), a wide area network (WAN), the Internet, a telephone line, a cable line, a radio

25   channel, an optical communications line, and a satellite communications link. Possible communications protocols that may be part of the system include: Ethernet (or IEEE 802.3), SAP, ATP, Bluetooth™, and TCP/IP. Further, networking of devices and computers may include use of 802.11b and related wireless protocols and/or use of cell networks (GSM and other emerging

30   standards).

In an embodiment, a central computer may not be necessary and / or preferred. For example, the present invention may, in one or more embodiments,

be practiced on a monitoring device in communication only with one or more user computers. In such an embodiment, any functions described as performed by the central computer or data described as stored on the central computer may instead be performed by or stored on one or more monitoring devices or user computers.

5

Processes

The following processes are described as routines performed by the central computer. However, it should be understood that such processes may be

10   performed entirely or in-part by other devices, such as those described herein.

Task registration process

Step 1: Receive task registration data.

15

Employing parties register at least one task with the central service by, for example, uploading data to the central computer from an employer device. Such data may be uploaded through a Web-accessible GUI, in accordance with Electronic Data Interchange (EDI) standards and formats, or the like.

20   Task data to be uploaded may include, but is not limited to: (1) IP addresses to patch through camera feeds, (2) remote file addresses for question content, possible answer choices and/or answer formats, (3) digital files containing information regarding question content and/or answer choice content, (4) financial data, such as compensation rates (for the central service and/or workers),

25   compensation instructions (e.g. payment medium/means) and/or an account number of the employing party (e.g. for automatic billing purposes), (5) instructions for completion of the task, (6) instructions for how a task is to be divided (e.g. an indication of the divisible units of a project), (7) instructions for how and/or when the complete task is to be returned and/or presented to the

30   employer, (8) required/desired worker qualifications (e.g. worker demographics), (9) performance conditions/prerequisites as defined herein.

Step 2: Process received task registration data.

In some embodiments, received task registration data is processed according to rules included therein or according to stored rules. For example, task
5   registration data may include a complete survey, and the survey may be divided into individual questions. Or, task registration data may include a complete document that needs to be proofread, and the document may be divided into pages, paragraphs, sentences, phrases or words.

Further, in some embodiments, received task registration data may be
10   divided into a given number of task instances according to a numerical minimum or maximum indicated by the employer. For example, an employer wishing to conduct a survey may indicate that questions are to be answered by at least 50 respondents (workers). In this case, a single question can be registered in a task database (described below) fifty times, as fifty separate micro-tasks.

15

Step 3: Store task registration data in task database.

Uploaded task data may be stored in a task database that is consulted in the below-described work session process. An example task database is shown in
20   Table 3 below:

Task identifier	Project identifier	Employer identifier	Task description	Compensation	Performance conditions/ prerequisites
321321	55555	190357	Survey question at C://tasks.questions.55555.0001	$.02	None
321322	55555	190357	Survey question at	$.02	None

			C://tasks.questions.55555.0002		

TABLE 3

<u>Worker registration process</u>

5

According to some embodiments, workers may be required to register before they are permitted to participate in work sessions.

Step 1: Receive registration request from potential worker.

10   According to some embodiments, potential workers may log on to a website hosted by the central computer or otherwise log on to an online service (e.g. an ISP's home page), at which time they may send a request to register as a worker by, for example, clicking on a button.

15   *Step 2: Request registration data from potential worker.*

According to some embodiments, workers may be required to provide certain data to the central computer in order to participate in work sessions as workers. Such data may include (1) contact information (name, address, phone number, email address, etc.), (2) Social Security Number (SSN), (3) demographic

20   information (race, gender/sex, age), and/or (4) financial account identifiers (e.g. credit card account numbers, debit card account numbers, checking account numbers, etc.).

The central computer may prompt or otherwise request any or all of such data from the potential worker after Step 1. Alternatively, such data may be

25   previously registered with the central computer, as may be the case where the central computer is a computer operated by an Internet Service Provider and the

potential worker is already registered as a customer of online services. That is, consumers who are registered with the central service as a subscriber/customer may already have some or all of the requisite registration data on file with the central computer. (See, e.g., Examples 1, 2, and 3 above).

5   In some embodiments, the terms of a general confidentially or nondisclosure agreement may be provided to the worker for acceptance. That is, because some or all of the projects registered by an employer may contain sensitive, confidential information, workers may be required to agree not to disclose to third parties any information obtained by virtue of their participation in

10   work sessions. Thus, if an employer wishing to gauge consumer feedback about a new product packaging design were to register a survey featuring the new product design, workers employed to provide feedback about the design would be contractually bound to not disclose information about the design to third parties.

15   *Step 3: Determine whether potential worker is permitted to participate in work sessions based on stored rules.*

After the worker provides the necessary registration data to the central computer, the central computer consults stored rules (e.g. in a database) to determine whether or not the worker meets the general requirements necessary to

20   participate in work sessions.

For example, the central computer may refuse to register any potential worker who does not accept the terms of a nondisclosure agreement.

Or, the central computer may refuse to register any potential worker who does not reside within a certain geographical region. For example, a stored rule

25   may indicate that workers must be citizens of the United States, as indicated through the provision of a valid SSN. In this case, the central server may receive a nine-digit number from the remote potential worker, and consult a remote database to determine whether or not the number corresponds to a validly issued SSN.

Further still, the central computer may refuse to register any potential

30   worker under a certain age, as indicated by a database lookup based on a provided SSN. Such an embodiment may be desirable where local child labor laws limit work by individuals under certain ages. The central computer may optionally be

configured to access a local or remote database comprised of such jurisdictional age limits. The central computer could consult the database so that the appropriate age limit is retrieved which corresponds to the potential worker's place of domicile. An example of such a database is shown in Table 4 below:

State	Minimum working age
NY	16
LA	15
IL	17

5

TABLE 4

Also, the central computer may refuse to register any potential worker who does not provide certain information by, for example, populating certain fillable

10   fields of a Web page. For example, state and federal equal opportunity and/or labor laws and regulations may require the operator of the central computer to record the age, race and gender/sex of each potential worker, in which case any potential workers failing to provide such information may be returned to a previous step in the process (e.g. so that the required information can be provided), or the

15   session may end.

Furthermore, in some embodiments, stored rules may require that the user meet certain minimum hardware requirements. That is, the system may require that user devices be capable of a certain minimum amount of functionality. For example, the system may require that a user device be configured to communicate

20   with the central computer through a modem of a certain speed, that the user device comprise a processor of a certain speed, etc.

Step 4: Create record for worker in worker database.

A record for the worker is created in a worker database including at least

25   some of the received registration data. According to some embodiments, a worker identification number may be assigned to the worker and stored in the worker's record. The worker database may be read from and/or written to by the central

computer during the below-described work session process.

An exemplary worker database is shown in Table 5 below:

Worker identifier	Work er passw ord	Worker name	Worker address	Worker email address	Desired form of payment/ Worker financial account number	Completed, uncompensated tasks	Total compen sation due	Total hours worked within last 24 hours	Total hours worked within last 30 days
222	Fish	Bill Jones	2 Main Street, Town, NY, USA	bjones@ emailsite .com	Check	Task identifiers: 321321, 321322	$.04	.00146	.00146

5   TABLE 5

Work sessions

Step 1: Receive request to initiate work session.

10   Registered workers can initiate work sessions without having previously

scheduled a work session. Such flexibility allows registered workers to log on at

any time and earn money by performing micro-tasks.

The request to initiate a work session can be communicated by the worker

in many ways, including but not limited to (1) using a mouse or other device

15   peripheral to the user computer to click on an area of a graphical user interface,

such as a Web page, hosed by the central computer, or (2) using a handheld

wireless device such as a cellular telephone to transmit dual-tone multi-frequency

(DTMF) tones to an Interactive Voice Response Unit (IVRU) operatively

connected to the central computer.

20   In some embodiments, the central computer may at this point request

and/or receive a worker identifier and/or password for security purposes.

Step 2: Determine if request to initiate work session is valid.

The central computer then determines if the received request to initiate a work session is valid. In some embodiments, the central computer may validate the request by simply checking the received worker identifier and/or password

5   against the worker database to determine if they correspond to a valid record.

Further, in some embodiments, the central computer may validate the request to initiate a work session by determining whether or not the worker is attempting to initiate a work session from an unauthorized location or using unauthorized equipment. For example, various employers may wish to prevent

10   their employees from performing tasks for other employers (by participating in work sessions) during regular working hours. As such, an employer may register with the central computer so that workers *cannot* participate in work sessions using company computers. Thus, an employer may register the IP addresses or machine identifiers of personal computers in its corporate network. Upon receiving a

15   request to initiate a work session, the central computer may then consult a database comprised of such identification information to determine whether or not the worker is attempting to initiate a work session from an unauthorized location or machine. If so, the central computer may determine that the request to initiate the work session is invalid, and may terminate the process at this point. An exemplary

20   database comprising prohibited employer devices is shown in Table 6 below:

Employer	Device identifier	Work session participation rule(s)
ABC Corporation	1234.1234.1234.1234	Not to be used in work sessions
ABC Corporation	1234.1234.1234.1235	Not to be used in work sessions
XYZ Ltd.	4321.4321.4321.4321	Not to be used in work sessions between 8AM and 6PM EST.

TABLE 6

In some embodiments, the step of validating a request to initiate a work session may include the step of determining whether or not a given worker has
5   surpassed a given work limit or compensation limit.   The operator of the central controller may wish to limit the amount of work that can be done within a certain period of time in order to comply with federal or state labor laws or regulations. For example, a given law may dictate that workers in the relevant jurisdiction may not work for more than 16 hours per day. In this case, the central computer would
10   consult a worker's record in the worker database and determine if the worker has performed more than 16 hours of work within the last 24 hours, and if so, the central computer may determine that the request to initiate the work session is invalid, and may terminate the process at this point. It should be noted that such a time limit may also be desirable in settings where the operator of the central
15   controller wishes to preserve the independent contractor status of workers by limiting the amount of hours available to workers.

Alternatively or additionally, the operator of the central controller may wish to limit the amount of compensation that can be earned by a given worker in a certain period of time. In this case, the central computer may be configured to
20   access a database that stores rules governing compensation limits, and may consult such a database and the worker database to determine if a given worker has surpassed a compensation limit. If so, the central computer may determine that the request to initiate the work session is invalid, and may terminate the process at this point.

25

Step 3: Identify task in task database.

Once a request to initiate a work session is validated, the central computer identifies a task in a task database.
30   According to some embodiments, the central computer allocates a task to a worker by simply, in a serial fashion, selecting the next available task from the task database.

According to other embodiments, the central computer allocates tasks to a worker according to task performance conditions or prerequisites that are stored in a task database. Thus, the central computer may serially review records in a task database, searching for tasks for which the worker may be suitable.

5   For example, a rule may dictate that only workers from a certain geographical area may be routed a particular task. Alternatively or additionally, a rule may dictate that workers are not to receive tasks that they have already performed (e.g. so that a worker does not get asked the same survey question twice).

10

Step 4: Transmit task data to worker including task content and response options.

Once it is determined which task a worker will be routed, task data is

15   transmitted to the worker device. In some embodiments, the data that may be transmitted may include a textual description of the task and a plurality of response options (e.g. a question and several possible answers, such as "yes" or "no", or several multiple choice answers). Further, the task data may include digital files comprising images or sounds.

20   An enumerated list of several different types of tasks that may be registered by employers and performed workers is provided below (see section below entitled "Application Contexts").

Step 5: Receive selected response(s) from worker.

25

After the worker receives the task data, the worker performs the task and sends the central computer his or her response using the worker device. For example, after reading a question and reviewing the possible answer choices, a user may press a key on a worker device corresponding to a particular answer

30   choice, and thereby transmit the selected answer choice to the central computer.

Step 6: Evaluate received response(s) and process accordingly.

According to some embodiments, a fraud-detection subroutine may be executed at this point to ensure that the worker is actually making a bona fide effort to contemplate tasks and transmit thoughtful responses. That is, the system may evaluate received responses against a database of stored rules to ensure that the worker is not merely providing a repetitive, thoughtless set of responses (e.g. answering every question with a "yes" response). Several methods for ensuring worker attentiveness are disclosed more fully with reference to Applicants' U.S. Pat. No. 6,093,026 entitled METHOD AND APPARATUS FOR ADMINISTERING A SURVEY, issued July 25, 2000, the entirety of which is incorporated by reference herein for all purposes.

Step 7: Adjust worker rating based on evaluation of received response(s).

In embodiments implementing fraud-detection methodology, a worker rating may be adjusted to reflect the worker's attentiveness and care in answering questions. Systems and methods for updating a worker rating based on a user's degree of attentiveness are described with reference to U.S. Pat. No. 6,093,026.

Step 8: Determine if a session termination rule is met. If not, return to Step 3. If so, proceed to Step 9.

Next, the central computer determines if a stored session termination rule is met. If a session termination rule is met, the process continues to Step 9. If not, the process returns to Step 3, where the worker would continue participating in the work session.

In one embodiment, the central computer makes this determination periodically. In another embodiment, the central computer makes this determination continuously or substantially continuously. Further, according to some embodiments, the central computer makes this determination in response to a worker request. That is, in some embodiments, a worker may unilaterally end his

or her participation in a work session by transmitting to the central server a signal indicating the desire to do so. The ability to terminate work sessions unilaterally adds flexibility to work sessions, and allows for the performance of micro-tasks at traditionally unconventional times.

5   In some embodiments, session termination rules may constitute time limits for work sessions to ensure that a worker does not work for more than a certain amount of time within a certain period. Such rules may be desirable in contexts that do not permit continuous work for a certain period without a break. For example, laws, regulations, and/or labor contracts may dictate that a break must be

10   given for every 8 hours of work. Or, as workers may be performing micro-tasks by operating worker devices such as personal computers, concerns about eye-strain, carpel tunnel syndrome, or other types of fatigue may necessitate a session termination rule that ends sessions after a predefined amount of time. Such rules would force a break in the continuity of a work session once the time limit has

15   been reached. Further, session termination rules may dictate that sessions terminate once workers demonstrate a marked change (i.e. deterioration) in performance. For example, if a worker's average response time (the time between the transmission of task data and the receipt of a response) increases beyond a certain threshold during a work session, a session termination rule may be

20   triggered. Or, if a worker's provided responses indicate a lack of attentiveness as discussed with reference to U.S. Pat. No. 6,093,026, a session termination rule may be triggered.

Alternatively or additionally, session termination rules may constitute compensation limits to ensure that a worker does not earn more than a certain

25   amount of compensation within a certain period. For example, once a worker has earned enough to pay for a currently outstanding service bill (e.g. a bill for cable or ISP services), a session may terminate. Such a rule would be desirable where the operator of the central service does not wish to compensate workers in cash, but would rather limit compensation to an offsetting of an outstanding bill for services.

30

Step 9: Calculate and initiate provision of compensation to worker based on session data.

Timing:

After a work session, the central computer system may determine the amount of compensation due to a worker and initiate the provision of compensation. In some embodiments, this step is initiated immediately following

5   the termination of a work session. In other embodiments, the calculation and provision of compensation is done periodically (e.g. weekly, monthly; at the end of a billing cycle). Further, in some embodiments, the calculation and provision of compensation could be performed by the central computer upon the worker's request (e.g. when a worker logs on and clicks a button to request payment to his

10   financial account on file with the central computer).

In some embodiments, payment may be withheld at this step if the transaction costs of providing compensation are not justified by the amount of payment. That is, because the embodiments of the present invention facilitate individually compensible micro-tasks, it may be desirable to have a determination

15   of when is most cost-effective to remit payment. For example, because it likely costs at least $.50 to process a credit to a credit card account, payment for micro-tasks may be withheld until there is at least $.60 of work performed by a given worker. An exemplary database follows that stores rules that may be used in determining when compensation due a worker sufficiently outweighs the

20   transaction costs of a particular form of payment:

Form of payment	Transaction cost	Required compensation due to justify payment
Credit card	$.50	$.75
PayPal	$.02	$.25
Check	$1.50	$1.55
Credit to ISP service account	$.00	$.01

TABLE 7

Calculation of payment amount:

In some embodiments, the central computer calculates pay rates based on

5   an advertised per-task rate. For example, if a worker performed 10 tasks priced at
$.10 each, the worker would have earned $1. Further, in some embodiments,
workers may be compensated at different pay rates according to their rating status.
For example, workers rated at "5" may receive a rate of $.02/question, while
workers rated at "4" may receive a rate of $.01/question. In such an embodiment,

10   the central computer would multiply the number of questions answered by the
given worker's pay rate.

Further, the step of calculating a payment amount may also include an
accounting for miscellaneous fees and charges. For example, the central computer
may reduce gross compensation due by various amounts including, for example:

15   (1) state and federal tax withholding amounts, (2) insurance premiums or co-pays,
and/or (3) past due or penalty amounts associated with a service account (e.g. ISP
or cellular phone service accounts).

Further still, the step of calculating a payment amount may also include a
credit for a "bonus" once a threshold amount of work has been performed (e.g.

20   every year, every X hours of work performed, etc.).

It should be noted that, in some embodiments, the step of calculating the
payment amount may take place before the optional step of determining whether or
not the transaction costs associated with the particular form of payment are
justified by the amount of payment due.

25

Payment mechanisms:

In some embodiments, after calculating the amount of payment due, the
central computer may initiate payment by instructing that an account associated
with the worker be credited. More particularly, in some embodiments, the central

30   computer may communicate with a remote server owned by a financial institution,
and may indicate an authorization to charge an account associated with the owner
of the central computer and credit an account associated with the worker.

In other embodiments, the central computer would initiate payment by crediting a service account associated with the worker. For example, where the central computer is operated by a provider of a service, such as an Internet Service Provider, a cable TV service provider or a cellular telephone service provider, a

5   worker's service account may be offset by any earned compensation. Thus, in such embodiments, workers may offset their service bills by performing micro-tasks. However, such service providers may optionally limit the ability to earn compensation by providing that workers can only earn up to the amount owed to the service provider. Should workers earn less than is currently owed to the

10   service provider, the central computer may output a bill for the difference between the value of the services rendered and the amount of compensation due. Further, in some embodiments, workers may earn more compensation than they currently owe for services, and the difference can be credited to a future billing cycle.

15   Form of payment:

Many different forms or mediums of payment are contemplated. As discussed above, the central computer could credit to a financial account associated with the worker, including service accounts, credit accounts, checking accounts,

20   and the like. Alternatively, the central computer may authorize the provision of other forms of compensation.

For example, product manufacturers may "employ" customers of their products and compensate them with rebates. In other words, customers may "earn" a rebate or coupon by answering questions about a previously-purchased

25   product, providing feedback and the like. Aside from potentially collecting valuable consumer feedback and data, such a program may simply be a way to interact with a customer after a purchase, enhancing the customer's image of the product.

Alternatively, in another embodiment, workers may be compensated with

30   discounts on merchandise they have not yet purchased. In addition to serving as a vehicle for providing interested customers with discounts, such an embodiment would be a useful way to identify price-sensitive customers.

In another alternate embodiment, workers may be allowed to view premium content (e.g. sports games, concerts) for "free" if they perform micro-tasks. For example, in an embodiment where a worker initiates a work session by logging on to the central computer through his personal computer, the worker may earn

5 passwords or codes that allow the worker to view a premium sports event on a restricted-access website.

Further, in another embodiment, workers may be allowed to earn event tickets (e.g. tickets to concerts, sporting events) or travel vouchers (e.g. airline tickets).

10

Step 10: Aggregate and transmit responses to employing party.

Periodically or at the end of a project (i.e. once all the tasks associated with a single, common project are completed), the central system would transmit all

15 received responses associated with the project (potentially from many workers) to the employing party.

In one embodiment, the central system merely transmits the raw response data. In another embodiment, the central system could process the responses by preparing summaries, statistics, charts, graphs, or the like based on the received

20 responses. The operator of the central controller may optionally charge a fee to the employing party for such additional processing.

Step 11: Charge employer for work allocation service.

The central computer may then charge the employer for the services

25 performed by the remote workers. For example, the central computer may initiate a billing routine or charge a predetermined financial account associated with the employer. The amount charged to the employer may reflect (1) an amount of work performed by, or compensation paid to, workers and/or (2) a service fee.

30

Application Contexts

Many different types of tasks can be registered by employers and

performed by workers. Generally, low-skill tasks that can be performed in conjunction with the embodiments of the present invention include tasks whereby a worker must receive task data and select a response from a limited set of responses. For example, low-skill tasks used in embodiments of the present invention may

5   require workers to make "binary" (e.g., "yes" or "no") decisions, or to select from an otherwise limited set of possible responses (e.g. multiple choice answers). A list of various exemplary applications of embodiments of the present invention follow.

1.   Opinion Polls and Research.

10   a.   Product packaging. In some embodiments, consumer products manufacturers, such as Proctor & Gamble, may employ workers to provide their opinion as to product packaging (e.g. "Which packaging do you like better, A or B?").

                      b.   Product rating/prescreening. In some embodiments, workers may
15   be asked simple binary (i.e. "yes or no", "like or dislike") questions about their feelings toward certain products. For example, workers could quickly rate greeting cards ("insincere?" … "offensive?"… "pushy?").

                      c.   Advertisement/commercial rating. In some embodiments, workers
20   may be asked to rate which of two advertisements or commercials they like better.

                      d.   Broadcast media rating/feedback. Similarly, in some embodiments, workers may be asked to rate TV pilot programs or provide input that may be useful in making programming decisions ("like or
25   dislike?", "which program would you watch if they were on at the same time, A or B?").

                      e.   Product configuration. In some embodiments, workers could rate comparative options for how products are best configured. For example, large restaurant chains could employ workers to help
30   identify which food items are best served together. Likewise, quick service restaurants could employ workers to define what constitutes a valuable "value meal", since consumer perceptions of value

constantly change, especially in light of competition.

    f.   Product placement. In some embodiments, workers may provide feedback as to the proposed placement of items in retail stores or in advertisements. E.g. a worker may be asked to select from a plurality of images the setting in which the Coke bottle first became apparent to them.

    g.   Public Relations: word, phrase or speech rating. Similarly, in some embodiments, corporations, politicians and other public figures may use embodiments of the present invention to test for negative/positive connotations and effects of words, phrases, or speeches. E.g. a question may ask: "Which phrase do you prefer: (A) "tax refund" or (2) "tax rebate?"

    h.   Simple, ad hoc surveys. In some embodiments, an employer can use the inventive system to administer quick surveys about any topic, provided that the responses are limited to simple selection of relatively few possibilities. For example, a lifestyle-oriented magazine may utilize the system to conduct a "hot or not?" survey. Or, news organizations may use the system to broaden the base of potential respondents on particular survey questions.

    i.   Lie detection. In some embodiments workers could watch testimony, speeches or the like and decide whether or not someone is "lying" or "telling the truth". For example, trial lawyers may wish to use the inventive system to see how a mock jury would react to a potential witness. Likewise, politicians may test the sentiment of the voting populous or a relevant constituency as to his or her stated version of a particular newsworthy issue/scandal.

    j.   Appearance evaluation. In some embodiments, employers may post images for review by workers. Thus, a lawyer may post two digital images of a potential witness (e.g. a criminal defendant) wearing different outfits, hairstyles, etc. Workers may then earn compensation by providing their opinion as to which of the two makes the potential witness appear more credible.

2. <u>Quality Control.</u> In some embodiments, businesses may utilize the inventive system to ensure quality of their products.

   a. <u>Manufacturing.</u> In some embodiments, workers can be employed to monitor images of assembly-line instances for early problem detection, potentially saving manufacturers from downstream costs associated with remedying problems. For example, a monitoring device such as a digital video camera, in conjunction with image-analysis software, may be employed to scan the mundane operation of an assembly line and route images of nonconforming events (i.e. images of product line instances that do not conform to a reference image) to workers for evaluation. Alternatively, workers may simply watch feeds or images of the assembly line themselves, reporting nonconforming/problem units as they are generated.

   b. <u>Package assembly.</u> In some embodiments, workers may monitor images captured by monitoring devices at warehouse operations to ensure that packages contain all invoiced items before they are shipped. For example, for each box of items to be shipped, an image could be captured (e.g. a top view of the box so as to make the boxes' contents apparent). Both the image and a list of invoiced items could be transmitted to a worker. The list of items and the image may appear on the worker's screen, and the worker could simply check off each item on the list if it is included in the box.

   c. <u>Cleanliness.</u> Employers may utilize embodiments of the present invention to monitor the cleanliness of physical settings such as businesses, parks, etc. Thus, in some embodiments, workers could monitor images taken from monitoring devices at restaurants and kitchens to verify that kitchens are clean, that food is prepared in a healthy, clean manner, and the like by watching the preparation process and reporting potential problems (e.g. by reporting "clean" or "unsanitary").

3. <u>Support for Artificial Intelligence Systems.</u> Although artificial intelligence is increasingly used in daily life, a major problem preventing further

utilization is its accuracy. Thus, in some embodiments, the present invention could be used to bolster the accuracy of such systems. In other words, workers could provide back-up support and error-checking for most any artificial intelligence system. For example:

5   a. Assistance with speech and handwriting recognition. Currently, prior art speech-to-text conversion software is, at best, 95% accurate. Prior art handwriting recognition software is similarly inaccurate. Thus, in some embodiments of the present invention, executives, lawyers and others using speech and handwriting

10   recognition could utilize the inventive system to have documents checked for accuracy. Simply, workers could just respond to different portions of text by informing the system if there is an "error" or "no error". In one such embodiment, workers could compare text to supposedly-corresponding voice files and indicate

15   "match" or "no match". In an alternate embodiment, workers could just read portions of text and answer "correct" or "error".

      b. Detection of unusual account activity. Currently, financial institutions employ algorithms to determine whether or not account activity is unusual. However, detected activity is often not

20   representative of a security problem (e.g. when a cardholder is on vacation, an account may be inappropriately disabled merely due to a large volume of purchases), and conversely, fraudulent activity often goes undetected. Thus, in some embodiments, transaction data is parsed and redacted to ensure anonymity (e.g. separated

25   from account numbers), and sent to workers to verify normality/abnormality of transaction patterns. Workers could respond by confirming whether or not a transaction pattern is "normal" or "abnormal".

      c. Automated customer service. Embodiments of the present

30   invention may be used to confirm the appropriateness/accuracy of automated customer service responses. For example, where software is employed to scan customer emails and provide

responses based on keywords therein, workers could read the proposed responses before they are sent to customers, and thereby confirm whether or not proposed automated responses squarely address the corresponding customer issues.

5   4. <u>Retail Assistance</u>. Generally, retailers may use the inventive system to:

      a. <u>Spot undetected customer issues.</u>

          i. <u>Customer dissatisfaction/satisfaction.</u> In some embodiments, workers can view images of retail customers to determine if they are satisfied or dissatisfied with

10   services. This information can be useful in determining how to allocate customer service representatives, and where to focus business resources generally. Such an embodiment is desirable because customer satisfaction often can be determined based on nonverbal signals, which are best

15   detected and interpreted by human monitors (e.g. facial expressions, body movements).

      b. <u>Spot undetected employee issues, assist with HR functions.</u>

          i. <u>Poor service.</u> In some embodiments, workers can be employed to (1) view images taken from monitoring devices

20   of retail employees as they serve customers and (2) report bad service. Also, workers can be employed to monitor when customers are *not* getting served. For example, a worker might simply click a button on a user device when a given customer "needs service", such as when a customer

25   appears confused, when they have been wandering the store, when they have been looking at a store directory or map, when they have been reading a product label for a long period of time, etc.

          ii. <u>Employee theft.</u> In some embodiments, workers can be

30   employed to view images, taken from monitoring devices, of retail clerks as they operate cash registers or otherwise handle employer assets. Workers could report "theft" or

"OK" for each transaction, and could thereby perform a very useful function in detecting fraud or theft (e.g. "skimming" of the cash register).

    iii. <u>Employee rating.</u> In some embodiments, consumers employed as workers could simply watch images of employees and rate them as "good" or "bad" and/or provide simple feedback inputs as "fire," "retrain," or "promote".

  c. <u>Spot undetected operational issues and assist routine operations.</u>

    i. <u>Inventory monitoring.</u> In some embodiments, workers may view images of a retailer's shelves, and report "sufficient inventory" or "out of stock".

    ii. <u>Age/ID Verification.</u> In some embodiments, workers may be transmitted camera images taken from already-in-place security cameras at convenience stores and simply determine whether each customer "looks" a certain age or not. Further, in such embodiments, the capture and transmission of images may be limited to when certain products are purchased (tobacco or alcohol), as indicated by products' UPC codes. Thus, a worker could simply provide "over the shoulder" validation for a merchant's decision to sell an individual cigarettes by selecting either "at least 18" or "under 18" after viewing the individual's image. Similarly, workers could view entrances (e.g. gates, doors) of certain age-restricted venues such as bars, events, etc.

5. <u>Environmental Monitoring.</u> In some embodiments, governmental or not-for-profit groups may employ workers to monitor images to determine environmental and agricultural problems as they develop. For example, workers could compare images taken every two weeks to determine if a given crop appears to be diseased, or if a given natural resource is deteriorating.

6. <u>Municipal/Local Law Enforcement.</u> In some embodiments, municipalities and local law enforcement agencies may employ workers to view images

taken from remote monitoring devices and review such images:

 a. <u>Public areas.</u> Parks and other public areas (e.g. street corners) may be monitored for suspicious activity. Simply, workers could simply view images and report "no problem" or "problem."

5 b. <u>Parking.</u> Workers could act as remote "meter maids" by viewing images of parking spots and indicating whether there is a "violation" or "no violation."

 c. <u>Moving violations.</u> Workers could view images of intersections and confirm moving violations (e.g. if a car ran a red light).

10 7. <u>The Internet.</u> The following embodiments may be particularly attractive to an Internet Service Provider who owns and operates the central computer.

 a. <u>Development of the World Wide Web, or certain "communities" therein.</u>

  i. <u>Rating of Websites.</u> In some embodiments, workers who are customers of an ISP rate websites by clicking a button on a graphical user interface (e.g. a browser) indicative of a selected rating. Workers could rate sites quickly for general quality/appeal (e.g. one to five "stars"), for age-appropriateness (e.g. PG, R, X; or just "child safe" or "adults only"), etc. The ISP's central computer could, in turn, average received ratings and publish them for customers to see (e.g. "This site's average user rating is 3.")

  ii. <u>Categorizing web sites.</u> In some embodiments, workers may be charged with the task of viewing a web site and selecting an appropriate category label (e.g. news, arts, special categories). Then, within categories, workers could sub-categorize to add further specificity (e.g. Connecticut news, national news, etc.). Ultimately, the central computer could use such "metadata" in performing Web searching and navigation (i.e. in determining relevant search results).

  iii. <u>Linking of web sites.</u> In some embodiments, the central computer (e.g. ISP server) can present workers with two

websites (e.g. in separate sub-windows), and workers can determine whether or not the two sites should be linked together by hyperlinks. Automatic selection of the two sites can be done randomly or quasi-intelligently (e.g. keyword-based).

b. Content previewing. In some embodiments, subscribers to an ISP service may pay a premium to employ a worker to make sure that minors (subscribers' sons and daughters) are not viewing inappropriate content, communicating with potentially threatening individuals, etc. In such an embodiment, workers could be routed Web pages, search results, or messages before a minor receives such content. The worker could be asked whether not such content is "appropriate" or "inappropriate" for a minor. If the content is appropriate, it could be transmitted to the minor. If the content is deemed inappropriate, the content would not be transmitted to the minor.

c. Human "Spam" filters. In some embodiments, as a premium service to ISP subscribers, workers may be employed to view email messages that initially appear to be unsolicited ("Spam") based on stored rules (e.g. if thousands of similar emails are simultaneously sent to other recipients from a single address). Such messages that appear to be spam could be deleted, marked, or sorted into a separate mailbox by workers. To ensure privacy, email addresses, names, addresses, phone numbers and other identifying information could be automatically redacted from messages.

8. Social.

a. Dating/matching assistance. In some embodiments, workers may rate potentially compatible dating candidates by viewing two pictures and/or textual profiles and selecting "compatible" or "not compatible."

9. Education.

a. Grading papers. In some embodiments, workers may log on and

correct papers or tests (e.g. spelling tests, multiple choice tests, etc.).

5   Additional Embodiments

       In some embodiments, workers may perform micro-tasks from their
       telephones while "on hold". For example, Tim Smith, a Verizon customer, calls a
10   customer service number for a computer problem he is having. While waiting on
       hold, Tim presses #123, which triggers an option that lets him earn money while he
       is on hold. While he is on hold, Tim proceeds to answer questions, and thereby
       earn compensation. However, his work session is terminated when a customer
       service representative picks up. Various embodiments for managing consumer-to-
15   consumer customer service while a first customer is waiting himself for customer
       service is discussed more fully with reference to Applicant's U.S. Pat. No.
       5,978,467, entitled METHOD AND APPARATUS FOR ENABLING
       INTERACTION BETWEEN CALLERS WITH CALLS POSITIONED IN A
       QUEUE, issued November 2, 1999, and U.S. Pat. No. 6,125,178, entitled
20   METHOD AND APPARATUS FOR ENABLING INTERACTION BETWEEN
       CALLERS WITH CALLS POSITIONED IN A QUEUE, issued September 26,
       2000, the entirety of which is incorporated by reference herein for all purposes.
       In some embodiments, individual users may post tasks to be performed by
       peers. That is, commercial or associational employers are not necessarily the only
25   types of employers that can benefit from embodiments of the present invention.
       Thus, an individual may seek a short answer to a particular question from an
       individual having similar demographic characteristics. For example, a high school
       student may wish to ask any other high school age student what is a good movie to
       take a date to on the upcoming weekend, and may indicate that she will pay $.25
30   for the answer. Thus, any high school student could respond with the answer (e.g.
       via a peer-to-peer communications system such as AOL's Instant Messenger) and
       thereby earn the offered compensation.

The following definitions are used herein below, unless otherwise indicated.

5   *Monitoring apparatus, monitoring device* - A device capable of receiving, via an
       input device, a signal and outputting the signal to a central computer and/or a user
       computer. In some embodiments, a monitoring apparatus may include (i) a
       processor, such as one based on the Intel® Pentium® series processor, and/or (ii) a
       data storage device/ memory. Example monitoring devices include those that are
10   capable of converting analog signals into digital data files. Such devices include,
       but are not limited to: (a) digital video cameras, (b) digital video cameras equipped
       with motion detection and/or "short loop" tripping features, and (c) digital
       cameras.

15   *Monitoring party, patroller, spotter, user, viewer* - A person who participates in
       the remote monitoring of sites, typically in exchange for compensation. In some
       embodiments, such persons are members of the public that have no prior affiliation
       with monitored sites. Thus, according to some embodiments, images and/or other
       data that is sent to such viewers for review is selected randomly or substantially
20   randomly, and/or may be edited (e.g. redacted) so that such viewers cannot
       determine the identity and whereabouts of particular sites. In this manner, the
       inventive system provides a secure method and system for allowing members of
       the public to, in an ad hoc manner, earn compensation for monitoring the security
       of private property.

25

       "No-man" zone - A security-sensitive area on a monitored site where no humans
       or vehicles should be monitored (e.g. no humans should be present).

       Site, remote site, property - Property, including but not limited to real property,
30   which is to be monitored. Such property is monitored by at least one monitoring
       apparatus.

Supervisor, trained professional, professional - An employee or agent of the
central computer's owner (e.g. Net Patrol). In some embodiments, supervisors
assist site owners in configuring and initializing monitoring devices.

5   *User computer, user device, device* - A device capable of (i) receiving a signal
from a central computer and/or a monitoring apparatus, (ii) outputting a signal to a
user (i.e. a viewer), (iii) receiving a response from a user via an input device, and
(iv) transmitting a signal indicative of the response to a central computer and/or a
monitoring apparatus. In some embodiments, a user device may include (1) a
10   processor, such as one based on the Intel® Pentium® series processor, and/or (2) a
data storage device/ memory. Example user devices include personal computers
and cellular telephones.

15   A. System configuration

1. Network embodiments

The embodiments described below can be configured to work in a network
20   environment whereby a central computer, a user (e.g. viewer) computer and/or the
monitoring device communicate with each other directly or indirectly, via a wired
or wireless medium such as the Internet, LAN, WAN or Ethernet, Token Ring, or
via any appropriate communications means or combination of communications
means. Communication between the devices and computers, and among the
25   devices, may be direct or indirect, such as over the Internet through a Website
maintained by a computer on a remote server or over an on-line data network
including commercial on-line service providers, bulletin board systems and the
like. In yet other embodiments, the devices may communicate with one another
and / or a computer over RF, cable TV, satellite links and the like.
30   In an embodiment, a central computer may not be necessary and/or
preferred. For example, embodiments of the present invention may, in one or more
embodiments, be practiced on a monitoring device in communication only with

one or more user computers. In such an embodiment, any functions described as performed by the central computer or data described as stored on the central computer may instead be performed by or stored on one or more monitoring devices or user computers.

5

B. Processes

1. Site registration

10   Site owners and/or operators may initially register with the system in order have their sites monitored by viewers. It is contemplated that site owners will purchase camera and/or other monitoring device equipment from the operator of the central computer (e.g. Net Patrol), although it is possible that site owners may register other existing cameras and/or other monitoring devices with the central

15   computer.

In embodiments where monitoring devices comprise cameras such as video cameras, cameras and supporting peripheral hardware may have embedded computer devices and may support various standard internetworking and operating system protocols (e.g. embedded Linux chips that support HTTP, SSL, FTP, CGI,

20   Java, etc.). For example, cameras available from Axis® Communications, Inc. may be employed, including model 2420 series network cameras with infrared (IR) lenses, model 250-S MPEG-2 network video servers, and model 2191 audio modules. Infrared lenses may be desirable for low-light (i.e. nighttime) image capture.

25   In some embodiments, cameras may also be equipped with PTZ (Pan/Tilt/Zoom) mechanisms to facilitate remote adjustment of field of view, focus, and the like. Further, in some embodiments, cameras may be configured to support on-demand requests for static and motion images submitted by remote parties, such as site owners, viewers and supervisors.

30   It may also be desirable that cameras are weather-insulated as they may be located outdoors and subjected to extreme temperatures, wind and precipitation. Further, each camera preferably may have two independent circuits, so that if one

fails the other can serve as a back-up. Similarly, cameras may employ dual, redundant power sources, such that if one power source is unavailable, a back-up power source (e.g. batteries, generators, etc.) may be used. Indeed, in some embodiments, completely autonomous, free-standing image capture hardware may

5   be employed. Such hardware may use solar panels and high capacity energy cells for power, and may use cellular/satellite communications for networking.

In some embodiments, the inventive system will likely tie into/ride on existing alarm systems. In such embodiments, the camera hardware could be initially installed as part of the alarm system or could be subsequently added on as

10   a retrofit. In either case, a user installation process may entail remote communication with a Net Patrol representative (e.g. a trained professional). Alternatively, the cameras may be installed professionally.

After the site owners obtain suitable monitoring devices, site owners may register with the system by interacting with the central computer in accordance

15   with the following process steps.

b. Initial customer registration

In some embodiments, after cameras are installed, a registration

20   process may follow. For example, cameras may be addressed (IP) and
registered in database. Also, the central system may record the type of
room (e.g., bedroom), the security priority assigned to the room (e.g.,
bedrooms are more important than kitchen), and the times the camera is to
be active (e.g. only between 9AM and 5PM). Also, GPS coordinates may

25   be registered so that the system can later determine if the camera has been
moved or tampered with (e.g. the system may make periodic queries to
monitoring devices, and/or any change in position may trigger a checkup
process). Further, the system may require registration of the site's
postal/street address, a geographically relevant emergency dispatch number

30   (i.e. an emergency dispatch phone number corresponding to the site's local
area), and the phone number of a relative of the site owner.

c. Testing

After cameras are installed, a test sequence may ensue to verify visibility and identify coverage gaps. For example, a site owner may be asked to walk through his or her house and a supervisor could verify coverage/identify gaps. The test may be recorded so that there is a record of the area that the supervisor and/or his or her employer (e.g. Net Patrol) is responsible for.

Also, there may be periodic, remote tests of the cameras to ensure that they are working properly. This could be done at non-invasive times, such as when a conventional alarm system is set and occupants have left the house. This would minimize any perceived privacy intrusion.

Further, testing may entail establishing a threshold for motion detection (e.g. for use in embodiments where image transmission is to be triggered upon motion detection). In this manner, the system can be programmed to ignore non-threatening motion, such as a small pet's movements at the site owner's premises.

2. "Patrol" sessions/ service administration

a. Binary determinations

In some embodiments, patrollers may log onto a central computer to monitor registered sites. In one embodiment, users are asked to make simple binary determinations about images received from monitored locations (e.g. "yes" or "no" answers). For example, in some embodiments, users may be asked to make a simple determination of whether or not they see a person in an image. That is, in private property contexts, there may be "no-man zones" at certain times (e.g. night) and in certain places (e.g. pools). Site owners may register, with the central computer, which areas (e.g. by camera location) are "no man" zones at particular times. For example, where a site owner has 3 cameras installed at a site, the site owner may indicate that "Camera Number 1", which

happens to focus on the site owner's driveway, is a "no man zone" between the hours of 10:30PM and 5AM.

Similarly, certain "buffer times" may be registered with the central computer, indicating the times during which activity at a site is to be

5   disregarded. For example, the central computer may be programmed to disregard all images received when the site owner is enabling or disabling a conventional security/alarm system (e.g. within one minute from when a breach is first detected, thereby allowing the site owner one minute to provide the correct, disabling password or code).

10   Also, other helpful binary determinations may be made by viewers such as: (1) Are doors/windows open or closed? (2) Are the lights on or off? (3) Is the electricity on or off? (4) Does the address have phone service?

Indeed, the system can be configured to make binary determinations

15   of seemingly non-binary questions simply by asking a binary question and verifying a first set of responses against subsequent verification sets (that may be more specific). For example, a first set of questions about an image taken at a private residence may ask: "Is this home safe or not safe?" Respondents may have a "hunch" that there is suspicious activity afoot at

20   the site, and may respond by selecting the "not safe" option. Should a sufficient number of initial respondents similarly indicate "not safe", the system may (1) submit the same image/video clip to more users for verification, and/or (2) ask a more specific question ("Does it appear that the home is on fire? Yes or no?" Or, "Does it appear that an intruder is

25   present in the home? Yes or no?").

b. Session timing

In some embodiments, patrollers may be able to log on and log off of the

30   central controller at any time (e.g. may start and stop monitoring sessions unilaterally at any time). However, cameras at a particular site may be only operative at certain times. For example, the camera system may turn on whenever

the user turns on his or her alarm (or 30 seconds thereafter). Additionally or
alternatively, the camera system may be triggered if a certain event occurs, such as
if (1) security "hacks" or breaches are detected in related security systems (e.g., if
the company's computer system is being hacked, the Net Patrol camera system

5   may turn on), or (2) a noise/volume threshold is broken (e.g. by a scream or crash)
as detected by a microphone.

3. Management of patrollers

10   a. Qualifying patrollers

According to one embodiment, a process for qualifying patrollers (e.g.
training and testing) is facilitated by the central computer. Training may comprise
the communication of instructional information along with practice routines.

15 Testing patrollers may entail testing the particular viewer(s) capabilities (e.g.
attention level, vision, etc.) so that (1) those below a given threshold of
attentiveness/responsiveness are banned from the system or retrained, and/or (2)
content can be subsequently provided/transmitted in accordance with each
patroller's individual level of attentiveness/responsiveness (e.g. higher contrast,

20 higher resolution, more time on each image, etc.).
Further, qualifying patrollers may entail remote diagnostics of the
patroller's computer (e.g. processor speed, connection speed, video card capability,
screen resolution) so that the system can determine how to send images, which
images to send, etc. (Alternatively, software to be downloaded from the central

25 computer could have different settings for different hardware configurations.)

              b. Session initiation

In one embodiment, patrollers may simply log on to the central computer

30 for each monitoring session by providing a username and password. More
sophisticated embodiments may require coordination/attentiveness checks (e.g.
trace a pattern with mouse cursor, view sequences of test images).

c. Motivators and compensation

i. Payment

5

In the simplest version, patrollers would be compensated in cash.

Similarly, patrollers may be able to earn their way out of debt (credit cards,

mortgages; banks could have borrowers monitor other mortgaged properties in the

bank's portfolio).

10

ii. Game themes, prizes

Monitoring sessions could take the form of several games that can motivate

and encourage patrollers to participate and pay attention. Such games may be

15   comprised of the following characteristics and features:

Patrollers may be rated and rewarded based on performance (e.g. reporting

of false positives).

Patrollers may be encouraged to pay attention by participating in a game

that asks them to spot objects embedded in or superimposed on an image (e.g. spot

20   and collect game pieces).

Homeowners and business owners (e.g. customers of Net Patrol) could post

bounties as rewards for reporting certain events, behavior, etc.

In a "team play" embodiment, ad hoc groups may see the same image, and

channel for discussion may open up (e.g. AOL Instant Messenger) so members can

25   confer as to image content.

In a slot machine themed embodiment, the transmitted images can form the

reels of slot machine. If the images are different, the patroller may win a prize.

Such an embodiment would encourage patrollers to pay close attention to the

content of the transmitted images.

30

d. Routing of video feeds and images; security features

Video feeds and images may be routed to particular patrollers (1)
randomly, (2) based on simple geographical constraints (e.g. different zip codes),
5   (3) based on patroller history (e.g. never the same location twice), (4) based on
customer (i.e. site owner) preferences (e.g. patrollers who are family members
first; levels of expertise).

A related embodiment entails the editing/redacting of images and feeds to
ensure anonymity for security and privacy purposes. For example, portions of an
10   image may be blurred or otherwise concealed to protect sensitive aspects of the
image.

e. Security breach procedures

15   Should a patroller detect a potential problem (e.g. a potential intruder), a
process for managing and escalating the response would be triggered. For
example, if the patroller detects a potential intruder, a two-way audio/video
communication channel may open up between the patroller's user device and the
monitoring device (or another device located at the monitored site) so that the
20   patroller can initiate a "stand down" procedure, asking challenge/response
questions (e.g. "what's the password?") to determine whether clearance should be
granted or whether emergency sequences should be initiated. Emergency
sequences can include simply allowing an alarm to be triggered or the direct
dispatch of emergency responders.
25   Alternatively, such a "stand down" procedure can be facilitated/managed
by the central computer system. For example, the central computer may transmit,
to an output device at the site, a prompt for a password. The central computer may
then receive a voice file from a person at the site (e.g. via a microphone), and
interpret the content of the voice file using voice recognition software. The
30   content of the voice file may then be compared to a stored password. Should the
provided password be incorrect, or should no password be provided within a
default time period, the central computer may initiate one or more emergency

sequences, such as those described herein. It should be noted that such an automated stand down procedure may also be implemented in conjunction with the systems and methods disclosed above

If a potential emergency is verified by a viewer and/or by the central
5   computer pursuant to the above-described processes, images may be sent to a device of the site owner (e.g. a site owner's cellular phone, personal digital assistant, personal computer, television, etc.) for confirmation before a first responder is dispatched. In some embodiments, the site owner may confirm any potential problem by providing a response. For example, a site owner may receive
10   an image on his cellular phone, and may be prompted to "press 1" if the person in the picture is not authorized to be at the premises. In this manner, by having the site owner involved in the monitoring session, false alarms may be reduced or virtually eliminated.

If a potential emergency is verified by a viewer and/or by the central
15   computer and/or by the site owner, the images/feed may be made available to first responders (e.g. police, firemen, first aid workers, etc.) for assistance in dealing with the emergency. For example, responders may use the images/feed to determine where perpetrators are hiding in the house/business, where a fire is burning, whether anyone is left on a floor or in the building, etc. Similarly, as
20   discussed more fully below, an audio communication channel may be opened to the occupants on the premises so that a customized, threat-specific evacuation plan can be communicated (e.g. "go out the back door") via a monitoring device or other device located at the site. Ultimately, the system may be used to prove the response activities of local responders (timing, procedures used, etc.).
25

f. Pricing

The site owner may pay for different degrees of service based on many metrics and service levels, including but not limited to, (1) artificial
30   intelligence (AI) based prescreening sensitivity, (2) the number of cameras, (3) the frequency of image transmission, (4) the number of images that are transmitted, (5) the number of images that are transmitted until a site owner

responds, (6) the number of patrollers, and (7) session times (e.g. a "vacation only" service).

5   IV. Aspects and embodiments specific to consumer/home systems

A. Home security - protection against external attacks

1. Integration with existing alarm systems

10   A camera system for use with embodiments of the present invention may *supplement* a conventional alarm system by covering those aspects of a site (e.g. a house) that the conventional alarm is not configured to monitor (i.e. areas other than perimeters).

Alternatively, the system may *reinforce* a conventional alarm system.
15   Because conventional security systems suffer from chronic false alarms, the system may solve this problem by providing an intermediate confirmation step before alarm signals are transmitted to responding authorities. That is, when a home alarm is tripped, the camera system may turn on so that one or more viewers can determine whether the alarm was triggered in response to a bona fide emergency.

20

2. "Real time" evacuation plans

In a home setting, there are many threats to guard against, including fire and burglary. Because patrollers would have a detached, "birds eye" view of the entire premises, operators of the system (e.g. Net Patrol) may offer to provide
25   "real-time" evacuation plans based on the threat. In other words, patrollers may come up with an "on the fly" evacuation plan to steer residents away from the dangerous areas (e.g. rooms on fire, rooms where the perpetrator is hiding) and send audio instructions (e.g. to speakers at the premises) on how to safely evacuate.

30

3. Privacy issues

Home security system customers may also be particularly concerned about privacy issues. Accordingly, there may be an initial, randomized pre-screening by trained professionals for sensitive images before they are sent to ad hoc patrollers for viewing. Further, to deter unauthorized distribution of images, transmitted

5   images may be watermarked or otherwise identified.

Likewise, home security system customers may be concerned about the ability of patrollers to use received images to plan a crime. Accordingly, as mentioned above, images may be transmitted randomly, based on geographical constraints, on a one-time-only basis, or the like.

10

B. Home monitoring - lifestyle/family-oriented systems

1. Elderly person monitoring product

15   *A related product for monitoring elderly people may aim to make sure that subjects are properly tended to (e.g. if they fall) and to make sure that subjects do not put themselves in dangerous situations (e.g. getting in the car, drinking, taking the wrong medication). However, such a product may be particularly susceptible to privacy concerns. Accordingly, images of elderly people may be digitally*

20   *modified so as to conceal identity (e.g. stock photo substitution for person's body or face; replacement of person's image with outline shape or avatar). Additionally or alternatively, elderly subjects may be assured that only "qualified" professionals (i.e. nurses) are watching the camera feeds.*

25   2. Child monitoring product

Similarly, a product for monitoring children would ideally serve the same purposes (safety). For example, because swimming pools can be "no man" (i.e. no child) zones at certain times (e.g. when parents are at work), the Net Patrol

30   system may be employed to monitor the pool. Similarly, the Net Patrol system may be used to monitor and prevent consumption of alcohol (e.g. cameras located by a liquor cabinet) and chemicals (e.g. cameras located under a kitchen cabinet).

Indeed, the Net Patrol system could work to make sure that teenagers or babysitters are not hosting parties at the residence (e.g. volume-based prescreening; quasi-binary decisions as discussed above).

        Indeed, the Net Patrol system may be applied to quality-ensure the work of

5   babysitters and day-care facilities. For example, patrollers may be asked to monitor "2 man zones" to confirm that at least 2 people are in the picture (i.e. that the babysitter is in the same room as the child). Likewise, patrollers may simply be asked to report whether inappropriate behavior is taking place (e.g. physical danger to the child).

10

V. Aspects and embodiments specific to business systems

        There may be specific service improvements uniquely designed for businesses. For example, patrollers may be employed to watch for and report theft,

15   thereby reducing shrinkage at retail establishments. Cameras can be set up to enable viewing of self-service check-out isles, the area underneath shopping carts, and employee backrooms. Indeed, the retailer may post a bounty to catch shoplifters.

20   VI. Additional embodiments

    A. Monitoring sessions (or at least short-loop portions thereof) may be recorded and stored for later reference (e.g. when an insurance claim is adjudicated, to prove emergency responder activity as discussed above,

25   etc.).

    B. If the customer's monitoring devices are not engaged, the operator of the system (e.g. Net Patrol) could not reasonably be held accountable because the system would not be activated. Accordingly, the central computer may email encrypted (e.g. time stamped) codes to customers to prove when its

30   on/off duty.

C. The system may be utilized in quasi-private property contexts (i.e. property where there are highly personal interests, but not necessarily real property ownership):

a. "Neighborhood Watch" embodiment: Cameras may be placed on neighbors' cars, on telephone poles, etc., and artificial-intelligence (AI) prescreening may be utilized to scan for apparently odd behavior, in which case feeds or images would be provided to patrollers for viewing. For example, AI could detect fire (e.g. via thermal-imaging) and where cars shouldn't be stopped/ "no standing zones" (e.g. via motion detectors).

b. School embodiment: Parents of both public and private schools students may pay patrollers (e.g. indirectly through Net Patrol) to monitor areas where children frequent with minimal adult supervision or areas where children are likely to be put in dangerous situations. For example, cameras may be put on playgrounds, in school busses, at bus stops, and the like to monitor for unscrupulous individuals (e.g. kidnappers, drug dealers, etc.) or dangerous behavior (e.g. altercations, drug use, etc.).

In one embodiment, after an initial set of Net Patrollers determines that a potential security breach is underway (i.e. that there IS a person in the picture), a series of images from the site are transmitted to one or more Patrollers who view the plurality of images and vote for/select the image that is most representative/useful of the potential security breach. For example, from a plurality of images containing a suspicious person, a Net Patroller may select the images that best show the person's face. The selected images are then sent to property owners, first responders, or the like, who may determine whether or not the person is authorized to enter the premises or not. Thus, in this embodiment, a whole series of images relevant to an "incident" are reviewed by Net Patrollers, and some of which may be forwarded to property owners.

In some embodiments, images from *several* cameras at the monitored site are transmitted to the property owner once a potential security breach is detected.

For example, cameras aimed at "approach zones" of a house (e.g. driveway, doorways) may provide images taken just before the potential security breach (i.e. such images may be temporarily stored via "short loop" in case such incident arises). In this way, property owners are provided with several incident-relevant

5   images for evaluation.

We claim:

1   1.   An apparatus comprising:
2   a plurality of image capture devices, each of which is configured to capture
3   images and to transmit captured images;
4   a node in communication with the image capture devices, in which the node
5   is configured to:
6   receive the captured images;
7   store the captured image;
8   associate each captured image with a respective location based on
9   its respective image capture device;
10   select at least one neuron;
11   transmit a first captured image to the at least one neuron;
12   receive a result from the at least one neuron;
13   determine whether the result indicates that a human is present in the
14 first captured image;
15   select at least one additional neuron based on whether the result
16 indicates that a human is present in the first captured image;
17   transmit the first captured image to the at least one additional
18 neurons;
19   receive at least one additional result from the at least one additional
20 neuron;
21   determine whether the at least one additional result indicates that a
22 human is present in the first captured image;
23   determine an alarm condition based on the at least one additional
24 result.

1   2.   The apparatus of claim 1, in which at least one image capture device is
2   configured to preprocess a captured images.

1   3.   The apparatus of claim 1, in which the node is further configured to
2   preprocess at least some of the captured images.

1   4.   The apparatus of claim 1, in which at least one image capture device is
2   configured to:
3   detect motion and
4   capture an image in response to detected motion.

1   5.   The apparatus of claim 1, in which the result received from the at least one
2   neuron is a one-bit indication of the result.

1   6.   The apparatus of claim 1, in which the result received from the at least one
2   neuron indicates one of
3   the presence of a human in the image,
4   the absence of a human in the image, and
5   uncertainty as to whether there is a human present in the image.

1   7.   The apparatus of claim 1, in which the at least one neuron has an associated
2   weight, and in which the node is configured to select the at least one additional
3   neurons based further on the weight of the at least one neuron.

1   8.   The apparatus of claim 1, in which the at least one neuron has an associated
2   weight, and in which the node is configured to determine an alarm condition based
3   further on the weight of the at least one neuron.

1   9.   The apparatus of claim 1, in which each neuron has an associated weight,
2   and in which the node is configured to adjust the weights based on based further on
3   the results.

1   10.   The apparatus of claim 1, further comprising:
2   a layer analyzer which is configured to allocate the neurons to different
3   layers, based on respective weights of the neurons.

1   11.   The apparatus of claim 1, in at least some of the image capture

2   device are arranged to capture images from areas in which human activity is

3   desired to be substantially nonexistent

1   12.   A method comprising:

2   receiving a captured images from a plurality of image capture

3   devices;

4   storing the captured image;

5   associating each captured image with a respective location based on

6   its respective image capture device;

7   selecting at least one neuron;

8   transmitting a first captured image to the at least one neuron;

9   receiving a result from the at least one neuron;

10   determining whether the result indicates that a human is present in

11   the first captured image;

12   selecting at least one additional neuron based on whether the result

13   indicates that a human is present in the first captured image;

14   transmitting the first captured image to the at least one additional

15   neurons;

16   receiving at least one additional result from the at least one

17   additional neuron;

18   determining whether the at least one additional result indicates that

19   a human is present in the first captured image; and

20   determining an alarm condition based on the at least one additional result.

1   13.   The method of claim 12, in which the result received from the at least one neuron indicates

2   one of

3   the presence of a human in the image,

4   the absence of a human in the image, and

5   uncertainty as to whether there is a human present in the image.

1 14.   The method of claim 12, in which each neuron has an associated weight,

2 and in which the node is configured to adjust the weights based on based further on

3 the results.

1 15.   An apparatus comprising:

2   a computing device in communication with a plurality of image capture

3 devices, in which the computing device is configured to:

4   receive the captured images;

5   store the captured image;

6   associate each captured image with a respective location based on

7 its respective image capture device;

8   select at least one neuron;

9   transmit a first captured image to the at least one neuron;

10   receive a result from the at least one neuron;

11   determine whether the result indicates that a human is present in the

12 first captured image;

13   select at least one additional neuron based on whether the result

14 indicates that a human is present in the first captured image;

15   transmit the first captured image to the at least one additional

16 neurons;

17   receive at least one additional result from the at least one additional

18 neuron;

19   determine whether the at least one additional result indicates that a

20 human is present in the first captured image;

21   determine an alarm condition based on the at least one additional result.

1   16.   A method comprising:

2   receiving a captured images from a plurality of image capture

3   devices;

4   storing the captured image;

5   associating each captured image with a respective location based on

6   its respective image capture device;

7   transmitting a first captured image to at least one neuron;

8   receiving a result from the at least one neuron;

9   determining whether the result indicates that a human is present in

10 the first captured image; and

11   determining an alarm condition based on the result.

1   17.   A method comprising:

2   receiving an image from an image capture device,

3   in which the image capture device generates an image of an area in

4   which human activity is desired to be substantially nonexistent;

5   determining information related to the area;

6   receiving a request for a first user to monitor;

7   receiving a user identifier;

8   verifying that the user identifier corresponds to the first user;

9   providing the first user with the image;

10   receiving a response to the image by the first user, in which the response

11 comprises an indication that a human is present in the image;

12   providing additional users with the image;

13   receiving responses to the image by the additional users;

14   evaluating the received responses;

15   determining, based on the information related to the area, an entity to

16 notify; and

17   notifying the entity.

1 18. The method of claim 17, in which the step of

2   determining information related to the area;

3   comprises

4   receiving a unique identifier from the image capture device;

5   accessing a record in a database using the unique identifier; and

6   determining, from the record, contact information for the area.

1 19. The method of claim 17, in which

2   providing the first user with the image;

3   comprises

4   transmitting the image to an internet protocol address which is

5 based on the first user.

1 20. The method of claim 17, in which

2   providing the first user with the image;

3   comprises

4   posting the image on a Web site.

1 21. A method comprising:

2   receiving a request for a first user to monitor;

3   verifying the first user;

4   providing the first user with an image of an area in which human activity is

5 desired to be substantially nonexistent;

6   receiving a response to the image by the first user; and

7   evaluating the received response.

1 22. The method of claim 21, in which the step of

2   verifying the first user

3   comprises

4   receiving an identifier; and

5   determining that the identifier identifies a prior registration.

1 23.   The method of claim 21, further comprising:

2   determining an attentiveness of the first user.

1 24.   The method of claim 23, in which the step of

2   determining an attentiveness of the first user

3   comprises

4   requesting that the first user respond to a false positive.

1 25.   The method of claim 24, in which

2   requesting that the first user respond to a false positive

3   comprises:

4   providing the first user with a false positive image;

5   receiving a response to the false positive image by the first user.

1 26.   The method of claim 25, further comprising:

2   determining whether the response to the false positive image indicates that

3   a human is present in the image.

1 27.   . The method of claim 23, in which the step of

2   determining an attentiveness of the first user

3   comprises

4   determining a reaction time of the first user.

1 28.   The method of claim 21, further comprising:

2   selecting the first user from a plurality of users.

1 29.   The method of claim 28, in which the step of

2   selecting the first user from a plurality of users

3   comprises

4   selecting the first user from the plurality of users based on the

5 image.

1   30.   The method of claim 21, further comprising:
2   providing at least one additional user with the image.

1   31.   The method of claim 30, in which the step of
2   providing at least one additional user with the image
3   is performed based on the response to the image.

1   32.   The method of claim 30, in which the step of
2   providing at least one additional user with the image
3   comprises:
4   determining, based on the response to the image, a number;
5   selecting a plurality of additional user, in which the cardinality of
6   the plurality is at least the number; and
7   providing the plurality of additional users with the image.

1   33.   The method of claim 21, further comprising:
2   determining a response time in receiving the response to the image.

1   34.   The method of claim 21, in which the response is one of:
2   an indication that a human is present in the image,
3   an indication that no human is present in the image, and
4   an indication of uncertainty whether a human is present in the image.

1   35.   The method of claim 21, in which the step of
2   evaluating the received response
3   comprises
4   determining, based on the received response, whether to notify an
5   entity.

1   36.   The method of claim 21, in which the step of

2   evaluating the received response

3   comprises

4   initiating a telephone call to a predetermined telephone number.

1   37.   The method of claim 21, further comprising:

2   adjusting a rating of the first user based on the received response.

1   38.   The method of claim 21, further comprising:

2   compensating the first user.

1   39.   The method of claim 38, in which the step of

2   compensating the first user

3   comprises

4   compensating the first user based on the received response.

1   40.   A method comprising:

2   a step for observing a plurality of images of an area in which human

3   activity is desired to be substantially nonexistent;

4   a step for ascertaining whether the plurality of images reliably indicates the

5   presence of a human in the area; and

6   a step for alerting an entity based on the step for ascertaining.

1   41.   A method comprising:

2   a step for assessing an area in which human activity is desired to be

3   substantially nonexistent; and

4   a step for alerting an entity based on the step for assessing.

1   42.   An apparatus comprising:

2   means for receiving images of an area in which human activity is desired to

3   be substantially nonexistent;

4   means for distributing the images for at least partial analysis;

5   means for calculating an analysis of the images; and

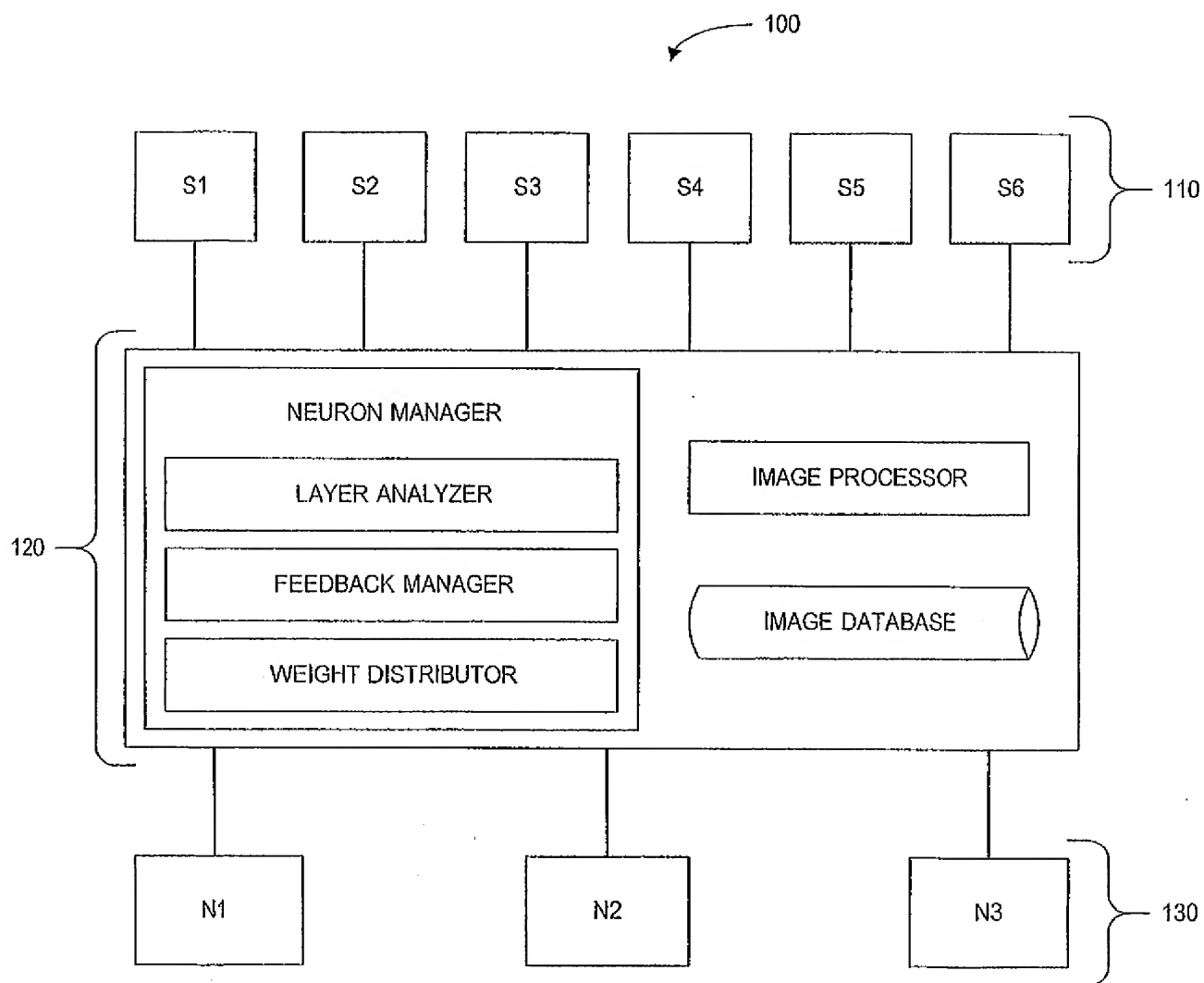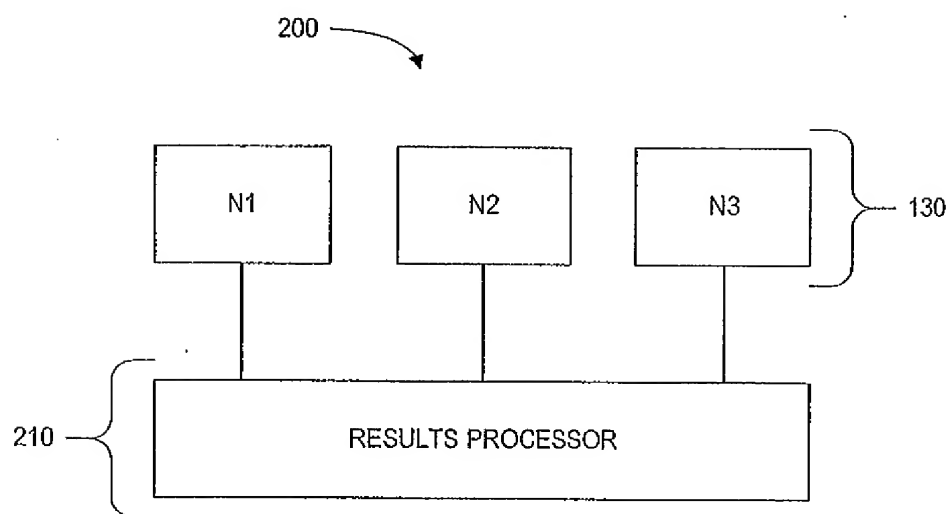6   means for warning an entity based on the analysis.

FIG. 1

200

N1   N2   N3   130

RESULTS PROCESSOR   210

FIG. 2